Universidad Autónoma de Madrid
Facultad de Ciencias
Departamento de Matemáticas

# Curvas Elípticas: Grupo de puntos racionales y curvas de rango alto

Enrique González Jiménez

Tesina dirigida por Adolfo Quirós Gracián

# Índice

# Introducción

El objeto de la Geometría Diofántica es el estudio de las ecuaciones diofánticas, es decir, el estudio de las soluciones racionales a ecuaciones polinómicas. En este empeño, dos ramas de las matemáticas nos proporcionan muchas de las herramientas necesarias: por un lado la Teoría de Números Algebraicos, que describe los anillos y cuerpos a los que estas soluciones pertenecen y, por otro, la Geometría Algebraica, ya que un sistema de ecuaciones polinómicas describe una variedad algebraica.

El caso más sencillo de ecuación diofántica es una ecuación polinómica en una variable,

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0.$$

Suponiendo que $a_0, \ldots, a_n$ son enteros, ¿cómo podemos encontrar todas las soluciones racionales de esta ecuación? La respuesta es sencilla, ya que si $(p, q) = 1$ y $x = \frac{p}{q}$ es una solución, entonces $p \mid a_0$ y $q \mid a_n$.

Cuando estudiamos ecuaciones en dos variables, la situación cambia totalmente. Dado un polinomio $f(x, y)$ con coeficientes racionales queremos estudiar las soluciones racionales de la ecuación $f(x, y) = 0$. Para ello se estudia el siguiente problema equivalente: encontrar las soluciones $[X, Y, Z] \in \mathbb{P}^2(\mathbb{Q})$ no nulas de la ecuación $F(X, Y, Z) = 0$, donde $F(X, Y, Z)$ es el polinomio que se obtiene homogeneizando $f(x, y)$. A partir de aquí nos podemos hacer las siguientes preguntas:

- ¿hay soluciones racionales?
- ¿cuántas hay?, en particular, ¿hay infinitas soluciones racionales?

El conjunto de soluciones $[X, Y, Z] \in \mathbb{P}^2(\mathbb{C})$ de la ecuación $F(X, Y, Z) = 0$ describe una curva en el plano proyectivo $\mathbb{P}^2(\mathbb{C})$. Para una ecuación lineal es fácil responder a nuestras preguntas, siempre hay infinitas soluciones racionales.

Para ecuaciones polinómicas de grado 2 es más delicado, pero no mucho más. Puede que no haya ninguna solución racional, pero si encontramos una, entonces tendremos infinitas. Mas aún, el Principio de Hasse-Minkowski nos dice que si tenemos un polinomio homogéneo cuadrático con coeficientes enteros, entonces tiene una solución racional no nula si y sólo si existe una solución real no nula y una en los números $p$-ádicos para todo $p$.

El caso de ecuaciones de grado 3 es totalmente distinto a los anteriores. En primer lugar no es fácil, en general, encontrar soluciones racionales como ocurría en el caso de ecuaciones lineales. Además, no se tiene un análogo al Principio de Hasse-Minkowski para polinomios de grado 3, como demostró Selmer ([SEL]) viendo que la ecuación $3X^3 + 4Y^3 + 5Z^3 = 0$ tenía una solución no nula en $\mathbb{R}$ y sobre los $p$-ádicos para cada $p$, pero ninguna solución racional.

Es el momento de presentar un importante concepto de la Geometría Algebraica, el género, que es un invariante de una curva. Las curvas que están definidas por polinomios de grados 1 ó 2 tienen género 0, por lo que son birracionalmente equivalentes a la recta proyectiva. Para curvas definidas por polinomios de grado 3 la situación cambia, ya que hay curvas que son birracionalmente equivalentes a la

recta proyectiva y otras que no lo son. Por lo que el grado no es buen criterio para clasificar las curvas; de ahí que hayamos introducido el género.

En el caso de curvas de género $> 1$ el Teorema de Faltings ([FAL1]) (anteriormente Conjetura de Mordell) asegura que el conjunto de puntos racionales de curvas de género $> 1$ es finito.

Para las curvas de género 1 todo lo anterior cambia, pudiéndose dar los tres casos, es decir, que no tengan puntos racionales, que el conjunto de puntos racionales sea finito o que éste sea infinito. De ahí que el estudio de curvas de género 1 sea el más interesante desde el punto de vista de la Geometría Diofántica. Nos limitaremos a estudiar aquellas curvas de género 1 que contienen algún punto racional, las llamadas *curvas elípticas*. La teoría de curvas elípticas es rica, variada, e increíblemente vasta. Además, esta teoría proporciona técnicas que pueden ser aplicadas con éxito al estudio de curvas de género mayor y de variedades (abelianas) de mayor dimensión.

Si tenemos una curva elíptica podemos introducir una operación y así dotar al conjunto de puntos racionales de la curva de una estructura de grupo abeliano. Esta operación, dada por el llamado método de las secantes y de las tangentes, fue introducida por Poincaré, aunque seguramente Fermat ya la conocía mucho tiempo atrás. Además Poincaré, en 1901, conjeturó que este grupo era finitamente generado; en 1923 Mordell lo demostró: si tenemos una curva elíptica $E$ y denotamos por $E(\mathbb{Q})$ al conjunto de puntos racionales de $E$, entonces $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$, donde $E(\mathbb{Q})_{tors}$ es el subgrupo de torsión de $E(\mathbb{Q})$, que es finito, y $r$ es el rango. La parte de torsión es fácil de calcular utilizando el Teorema de Nagell-Lutz. Además ha sido totalmente clasificada mediante el Teorema de Mazur. Sin embargo el rango no es tan sencillo de calcular, incluso para una curva elíptica dada. Menos aún se conocen los posibles rangos que pueden darse. Se conjetura que existen curvas elípticas de rango arbitrariamente alto. De ahí que esta memoria esté especialmente orientada a describir los últimos avances en la obtención de curvas elípticas de rango alto.

Las curvas elípticas adquieren gran interés en otras ramas de las matemáticas, como son:

- Estudio del número de clase de cuerpos cuadráticos imaginarios (en relación con la conjetura de Birch-Swinnerton-Dyer ([GOL])).
- Aplicaciones a la criptografía ([KOB]):
  - Factorización (H. W. Lenstra).
  - Primalidad (Atkins, Morain).
  - Criptosistemas basados en curvas elípticas (Koblitz).
- Último Teorema de Fermat (en relación con la conjetura de Shimura-Taniyama-Weil ([WIL])).

No hay ninguna pretensión de originalidad en la memoria, ya que todos los resultados son conocidos. Sin embargo, la memoria aporta algunas demostraciones que

no aparecen completas en la literatura y también alguna forma nueva de demostrar resultados conocidos, en particular en los capítulo 1 y 7.

En el primer capítulo veremos una serie de conceptos básicos de la teoría de curvas planas. En concreto, enunciaremos el Teorema de Bézout, que será fundamental en la teoría desarrollada en este capítulo. Estudiaremos las curvas definidas por polinomios cúbicos irreducibles de grado 3. Haremos un desarrollo cuidadoso y completo del que llamaremos "algoritmo de Weierstrass", así como un estudio completo de cuándo se puede aplicar. Es decir, veremos cuándo una curva cúbica irreducible puede ser expresada en una forma de Weierstrass. También haremos un estudio de las curvas dadas en una forma de Weierstrass, para así obtener una primera definición de curva elíptica.

Posteriormente consideraremos una operación (que daremos explícitamente) que dotará al conjunto de puntos racionales de una curva elíptica de una estructura de grupo abeliano.

El capítulo 2 recoge los resultados que necesitamos de los capítulos 1 y 2 de [SIL], aunque hemos desarrollado completamente algunos ejemplos y hemos incluido demostraciones de algunos teoremas que consideramos importantes y que no aparecen en [SIL]. Daremos una nueva definición de curva elíptica y comprobaremos que es equivalente a la formulada en el capítulo anterior.

El capítulo 3 está dedicado a la demostración del Teorema de Mordell. Hemos utilizado como modelo la demostración de [KNA] que tiene la ventaja de ser "elemental". Knapp demuestra completamente el caso en que $E(\mathbb{Q})$ tiene tres puntos de orden 2, y da una idea de cómo probarlo en general. En la memoria desarrollamos completamente este caso general. Por último, enunciaremos distintas generalizaciones de este teorema.

El capítulo 4 trata sobre el subgrupo de torsión de una curva elíptica definida sobre $\mathbb{Q}$. El resultado principal será el Teorema de Nagell-Lutz, que permite obtener explícitamente el subgrupo de torsión de una curva elíptica dada. Para su demostración introduciremos los números $p$-ádicos y la filtración $p$-ádica.

Se calcularán explícitamente los subgrupos de torsión de algunas curvas y familias de curvas. En el caso de las familias se utilizará la reciprocidad cuadrática, así como el Teorema de Dirichlet de los números primos en una progresión aritmética.

Enunciaremos el Teorema de Mazur que clasifica por completo los subgrupos de torsión de las curvas elípticas definidas sobre $\mathbb{Q}$. Por último consideraremos curvas elípticas definidas sobre cuerpos de números, resaltando los avances más importantes que se han hecho en torno a la Conjetura de acotación uniforme hasta llegar a su demostración por Merel. Queda pendiente el problema del estudio del rango, y a él están dedicados los tres últimos capítulos.

En el capítulo 5 veremos que el rango no es fácil de calcular en la práctica.

Se obtendrá una cota para él, que hacemos explícita en todos los casos ([KNA] se limita a curvas elípticas con 3 puntos de orden 2) en función de los primos de mala reducción. Veremos que para buscar curvas elípticas con rango alto habrá que considerar curvas elípticas con discriminante muy grande. Y que las curvas elípticas tienden a tener rango pequeño. De hecho se conjetura que el rango medio es menor que 1 ([B-M]). Brumer y McGuinness calcularon el rango para 310716 curvas elípticas (para todas las curvas elípticas definidas sobre $\mathbb{Q}$ de conductor primo $< 10^8$) y obtuvieron que el rango medio es 0.98.

El capítulo 6 está dedicado a enunciar algunas de las conjeturas más importantes de la teoría de curvas elípticas, como son la de Birch-Swinnerton-Dyer y la de Shimura-Taniyama-Weil. La primera nos es de gran interés ya que determina cúal es el rango de una curva elíptica (comentaremos los últimos avances realizados en torno a ella). También se enuncia una conjetura sobre la existencia de curvas elípticas de rango arbitrariamente grande.

El último capítulo es la parte principal de esta memoria, y está dedicado a las curvas elípticas de rango alto. En él se explican los métodos más relevantes que se utilizan para obtenerlas. Este capítulo está basado principalmente en varios artículos y trabajos de Nagao, Mestre y Fermigier.

En primer lugar, aportaremos una demostración detallada de por qué la criba que utiliza Nagao es una buena aproximación del rango. Para ello se supondrán ciertas las conjeturas de Birch-Swinnerton-Dyer y la de Sato-Tate. Con esta criba se obtendrán curvas elípticas de rango alto definidas sobre $\mathbb{Q}$.

Después haremos un breve estudio de las superficies elípticas, para obtener teoremas de especialización sobre éstas y así conseguir curvas elípticas definidas sobre $\mathbb{Q}(T)$ de rango alto. Aportaremos un resultado que nos asegura que si tenemos secciones dependientes en una superfie elíptica, entonces al especializarlas, obtenemos puntos dependientes en la especialización de la superficie elíptica en un determinado punto. Además, comentaremos un resultado de Silverman que asegura que el rango de la curva obtenida al especializar es mayor que el rango de la curva elíptica definida sobre $\mathbb{Q}(T)$ en casi todo punto. Así, construyendo curvas elípticas definidas sobre $\mathbb{Q}(T)$ de rango alto, tendremos muchas posibilidades de encontrar curvas elípticas definidas sobre $\mathbb{Q}$ de rango muy elevado.

Se define una nueva criba, también debida a Nagao, pero esta vez para curvas elípticas definidas sobre $\mathbb{Q}(T)$. Con ella enunciaremos la Conjetura de Nagao, y mencionaremos algunos casos en los que esta conjetura es verdadera.

En [MES1], Mestre proporciona un método para obtener curvas elípticas definidas sobre $\mathbb{Q}(T)$ de rango $\geq 11$ e incluye un ejemplo explícito. Nosotros detallaremos su prueba y daremos una nueva demostración que hace uso de la especialización de superficies elípticas.

Posteriormente explicaremos un nuevo método de Mestre, mucho más potente que el anterior, para obtener curvas elípticas definidas sobre $\mathbb{Q}(T)$ de rango al menos 12. Expondremos varios ejemplos, uno de Mestre de rango $\geq 12$ y otro de Nagao con rango $\geq 13$ (este último obtenido usando la criba para curvas elípticas

definidas sobre $\mathbb{Q}(T)$). Además daremos un ejemplo de una curva elíptica definida sobre $\mathbb{Q}(u,v)(T)$ de rango al menos 13.

Por último, consideraremos dos ejemplos de curvas elípticas definidas sobre $\mathbb{Q}$. El primero, de Nagao, define una curva elíptica de rango $\geq 21$; y el actual récord, debido a Fermigier, con una de rango $\geq 22$, obtenida a partir de la curva elíptica definida sobre $\mathbb{Q}(u,v)(T)$ de rango $\geq 13$ dada por Mestre.

Hay que resaltar que tanto Nagao como Fermigier, como Mestre hacen uso de computadoras de gran potencia para obtener estos ejemplos. Como se puede observar, los coeficientes y las coordenadas de los puntos son astronómicamente grandes, de ahí que se necesite usar computadoras capaces de manejar números de muchas cifras. En la memoria, varios de los cálculos se han realizado mediante computadoras, usando programas matemáticos especialmente orientados al manejo de grandes cifras, como es PARI. También se hizo uso del paquete APECS de MAPLE para el cálculo simbólico orientado a las curvas elípticas y del paquete Elliptic Curve Calculator para MATHEMATICA, con el que se obtuvieron las gráficas que aparecen en el capítulo 1.

Getafe, Madrid.
Enero de 1998.

# Capítulo 1

# Curvas cúbicas y curvas elípticas.

En este primer capítulo desarrollaremos técnicas básicas sobre curvas proyectivas planas. Su parte principal es el estudio de cúbicas irreducibles. Veremos cuándo una cúbica irreducible definida sobre un cuerpo $K$ tiene asociada una ecuación de Weierstrass.

Definiremos curva elíptica en estos términos. Veremos, además, como ésta tiene asociada una ley de grupo, que dota al conjunto de puntos racionales de una curva elíptica de una estructura de grupo abeliano.

## 1.1 Conceptos básicos.

En este primer apartado introducimos la noción de curva proyectiva en $\mathbb{P}^2(K)$, con $K$ un cuerpo algebraicamente cerrado (por ejemplo $\overline{\mathbb{Q}}, \mathbb{C}, \overline{\mathbb{F}}_p, \dots$ ).
**Notación**: Denotaremos por $\mathbb{P}^2$ al plano proyectivo $\mathbb{P}^2(K)$, definido sobre el cuerpo $K$; y por $\mathbb{A}^2$ al plano afín $\mathbb{A}^2(K)$.

**Definición.** *Sea $F(x, y, z)$ un polinomio homogéneo de grado $d > 0$ con coeficientes en $K$, sin factores repetidos. Se define la* **curva proyectiva plana** *$C$ dada por F(x,y,z) como*

$$C = \{[x, y, z] \in \mathbb{P}^2 : F(x, y, z) = 0\}.$$

**Definición.** *El* **grado** *de una curva proyectiva plana $C$, definida por el polinomio $F$, es el grado de $F$. La curva $C$ se dice* **irreducible** *si $F$ es irreducible.*

**Definición.** *Un punto $P = [x_0, y_0, z_0]$ de una curva proyectiva plana $C$, definida por el polinomio $F$, se dice* **punto singular** *si*

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0.$$

*Una curva se dice que es* **no-singular** (*o* **lisa**) *si no tiene puntos singulares.*

**Definición.** *La* **recta tangente** *a una curva proyectiva plana $C$, definida por el polinomio $F$, en un punto no singular $P \in C$ es la recta de ecuación*

$$\frac{\partial F}{\partial x}(P) \cdot X + \frac{\partial F}{\partial y}(P) \cdot Y + \frac{\partial F}{\partial z}(P) \cdot Z = 0.$$

**Definición.** *Sea $f(x, y)$ un polinomio de grado $d > 0$ con coeficientes en $K$. Se define la* **curva afín plana** *$C$ definida por $f(x, y)$ como*

$$C' = \{(x, y) \in \mathbb{A}^2 : f(x, y) = 0\}.$$

A partir de una curva afín $C'$ obtenemos una curva proyectiva $C$ añadiéndole a $C'$ "puntos en el infinito".

Si identificamos $\mathbb{A}^2$ con el abierto $U = \{[x, y, z] \in \mathbb{P}^2 : z \neq 0\}$ en la forma habitual, es decir, mediante la función

$$\begin{array}{rccc} \phi: & U & \longrightarrow & \mathbb{A}^2 \\ & [x, y, z] & \longmapsto & \left(\frac{x}{z}, \frac{y}{z}\right), \end{array}$$

cuya inversa es

$$\begin{array}{rccc} \phi^{-1}: & \mathbb{A}^2 & \longrightarrow & U \\ & (x, y) & \longmapsto & [x, y, 1], \end{array}$$

podemos relacionar una curva afín plana $C'$ con una curva proyectiva plana $C$.

El complementario de $U$ en $\mathbb{P}^2$ es la recta proyectiva definida por $z = 0$ que puede identificarse con $\mathbb{P}^1$ vía la aplicación:

$$\begin{array}{ccc} \{z = 0\} & \longrightarrow & \mathbb{P}^1 \\ [x, y, 0] & \longmapsto & [x, y]. \end{array}$$

Sea $F(x, y, z)$ un polinomio homogéneo de grado $d > 0$. Bajo la identificación de $U$ con $\mathbb{A}^2$ anteriormente descrita, la intersección de $U$ con la curva proyectiva $C$ definida por $F(x, y, z)$ es una curva afín en $\mathbb{A}^2$ definida por el polinomio en dos variables

$$f(x, y) = F(x, y, 1).$$

Si $z \not| F(x, y, z)$, el polinomio $f$ tiene grado d. Recíprocamente, si $f(x, y)$ es un polinomio de grado d, es decir,

$$f(x, y) = \sum_{i+j \leq d} a_{ij}\, x^i\, y^j,$$

entonces la curva afín $C'$ definida por $f(x, y)$ es la intersección de $U$ con la curva proyectiva plana $C$ definida por el polinomio homogeneizado

$$z^d\, f\left(\frac{x}{z}, \frac{y}{z}\right) = \sum_{i+j \leq d} a_{ij}\, x^i\, y^j\, z^{d-i-j}.$$

La intersección de esta curva proyectiva con la recta del infinito $z = 0$ es el conjunto de puntos

$$\{[x, y, 0] \in \mathbb{P}^2 : \sum_{0 \leq i \leq d} a_{i,d-i}\, x^i\, y^{d-i} = 0\}.$$

Por ser $K$ algebraicamente cerrado, se tiene que $\exists\ \alpha_i, \beta_i \in K$ tales que

$$\sum_{0 \leq i \leq d} a_{i,d-i}\, x^i\, y^{d-i} = \prod_{0 \leq i \leq d} (\alpha_i x + \beta_i y).$$

Llamaremos asíntotas de la curva afín plana $C'$ definida por $f$ a cada una de las rectas $\alpha_i x + \beta_i y = 0$. Cuando se identifica la recta $z = 0$ en $\mathbb{P}^2$ con un $\mathbb{P}^1$, estas rectas corresponden a los puntos $[-\beta_i, \alpha_i]$, que son precisamente los puntos de $C \backslash C'$.

**Observación 1.1.1** Hemos conseguido una correspondencia biyectiva entre las curvas afines $C'$ en $\mathbb{A}^2$ y las curvas proyectivas $C$ en $\mathbb{P}^2$ que no contienen la recta $z = 0$.

**Observación 1.1.2** Con las notaciones anteriores se tiene que

$$C \text{ lisa} \Longrightarrow C' \text{ lisa}.$$

El inverso no es cierto en general, ya que $C$ puede tener singularidades en la recta del infinito $z = 0$. Lo que si podemos decir es que si $C = \{[x, y, z] \in \mathbb{P}^2 : F(x, y, z) = 0\}$ es una curva proyectiva plana, entonces

$$[x_0, y_0, 1] \in C \text{ no singular} \Longleftrightarrow (x_0, y_0) \in C' \text{ no singular}.$$

con $C' = \{(x, y) \in \mathbb{A}^2 : F(x, y, 1) = 0\}$.

## 1.2 Teorema de Bézout.

En esta sección enunciaremos el Teorema de Bézout, un resultado básico en la teoría de curvas planas.

Sean $F(x) = a_0 + a_1 x + \ldots + a_n x^n$ con $a_0, \ldots, a_n \in \overline{K}, a_n \neq 0$, y $G(x) = b_0 + b_1 x + \ldots + b_m x^m$ con $b_0, \ldots, b_m \in \overline{K}, b_m \neq 0$, dos polinomios de $\overline{K}[x]$. Y denotemos por $\overline{K}_m$ al espacio vectorial de polinomios de $\overline{K}[x]$ de grado $< m$. Consideramos la aplicación

$$\begin{array}{cccc} \Phi & \overline{K}_m \times \overline{K}_n & \longrightarrow & \overline{K}_{m+n} \\ & (\varphi, \psi) & \longmapsto & F\varphi + G\psi. \end{array}$$

**Definición.** *Se define la* **resultante de** $F$ **y** $G$, $\mathcal{R}_{F,G}$, *como*

$$\mathcal{R}_{F,G} := det(\Phi).$$

Si tomamos la base natural de salida

$$(1,0),\ldots,(x^{m-1},0),(0,1),\ldots,(0,x^{n-1}),$$

y la de llegada

$$1,\ldots,x^{m+n-1},$$

deducimos

$$\mathcal{R}_{F,G}=\begin{vmatrix} a_0 & a_1 & \ldots & a_n & 0 & 0 & & & & \ldots & 0\\ 0 & a_0 & a_1 & \ldots & a_n & 0 & & & & \ldots & 0\\ \vdots & & \ldots & & & & \ldots & & & & \\ & & \ldots & & & & \ldots & & & & \vdots\\ 0 & 0 & \ldots & 0 & a_0 & a_1 & \ldots & & & \ldots & a_n\\ b_0 & b_1 & & \ldots & & \ldots & \ldots & b_m & 0 & \ldots & 0\\ 0 & b_0 & b_1 & & \ldots & & \ldots & & b_m & 0 & \ldots & 0\\ \vdots & & \ldots & & & & & \ldots & & & \\ & & \ldots & & & & & \ldots & & & \vdots\\ 0 & \ldots & 0 & b_0 & b_1 & & & & & \ldots & b_m \end{vmatrix}.$$

Si

$$F(x,y,z)=a_0(x,y)+a_1(x,y)z+\ldots+a_n(x,y)z^n$$

y

$$G(x,y,z)=b_0(x,y)+b_1(x,y)z+\ldots+b_m(x,y)z^m$$

son polinomios en las variables $x,y,z$, entonces la resultante

$$\mathcal{R}_{F,G}(x,y)$$

de $F$ y $G$ con respecto a $z$ se define de manera análoga al determinante $\mathcal{R}_{F,G}$ sustituyendo $a_i$ y $b_j$ por $a_i(x,y)$ y $b_j(x,y)$ con $i=1,\ldots,n$ y $j=1,\ldots,m$.

Antes de enunciar el teorema de Bézout debemos definir el número de intersección $I_P(C,D)$ en un punto $P=[a,b,c]$ de dos curvas planas $C$ y $D$. Si $C$ y $D$ están definidas por los polinomios $F(x,y,z)$ y $G(x,y,z)$, definiremos el número de intersección usando la resultante de $F$ y $G$ en un cierto sistema de coordenadas. Para ver que la definición es independiente de la elección de las coordenadas, vamos a mostrar que está unívocamente determinado por las propiedades enunciadas en el siguiente teorema.

**Teorema 1.2.1** *Hay un único número de intersección $I_P(C,D)$ definido para todas las curvas planas $C$ y $D$ que satisface las siguientes seis propiedades:*

*(i)* $I_P(C,D)=I_P(D,C)$.

*(ii)* $I_P(C,D)=\infty$ *si $P$ pertenece a una componente común de $C$ y $D$; en otro caso, $I_P(C,D)$ es un entero no negativo.*

*(iii)* $I_P(C, D) = 0$ *si y sólo si* $P \notin C \cap D$.

*(iv) Para dos rectas distintas el único punto de intersección tiene número de intersección igual a* 1.

*(v) Si* $C_1$ *y* $C_2$ *están definidas por polinomios homogéneos* $F_1(x, y, z)$ *y* $F_2(x, y, z)$ *y* $C$ *está definida por*

$$F(x, y, z) = F_1(x, y, z) \cdot F_2(x, y, z)$$

*entonces*

$$I_P(C, D) = I_P(C_1, D) + I_P(C_2, D).$$

*(vi) Si* $C$ *y* $D$ *están definidas por polinomios homogéneos* $F$ *y* $G$ *de grados* $n$ *y* $m$ *respectivamente, y* $E$ *está definida por* $FR + G$ *donde* $R$ *es un polinomio homogéneo de grado* $m - n$*, entonces*

$$I_P(C, D) = I_P(C, E).$$

*Demostración*: Ver [KIR], Teorema 3.18.

**Teorema 1.2.2** *Si* $C$ *y* $D$ *no tienen componentes comunes y si elegimos coordenadas proyectivas tales que satisfagan las condiciones*

*(i)* $[0, 0, 1]$ *no pertenece a* $C \cup D$*;*

*(ii)* $[0, 0, 1]$ *no pertenece a ninguna recta que contenga dos puntos de intersección distintos de* $C \cap D$*;*

*(iii)* $[0, 0, 1]$ *no pertenece a la recta tangente a* $C$ *o a* $D$ *en cualquier punto de* $C \cap D$*;*

*entonces el* **número de intersección** $I_P(C, D)$ **de** $C$ **y** $D$ **en** $P$*, con* $P = [a, b, c] \in C \cap D$*, es el mayor entero* $k$ *tal que* $(ay - bx)^k$ *divide a la resultante* $\mathcal{R}_{F,G}(x, y)$*. Es decir,*

$$I_P(C, D) = ord_{(ay-bx)}\mathcal{R}_{F,G}(x, y).$$

*Demostración*: Ver [KIR], Teorema 3.18.

**Teorema de Bézout.** *Sean* $C$ *y* $D$ *curvas proyectivas planas, de grados* $m$ *y* $n$ *respectivamente, sin componentes comunes. Entonces hay* $m \cdot n$ *puntos de intersección, contando multiplicidades. Es decir,*

$$\sum_{P \in C \cap D} I_P(C, D) = m \cdot n,$$

*con* $I_P(C, D)$ *la multiplicidad de intersección en el punto* $P$*.*

*Demostración*: Ver [KIR], Teorema 3.1.

**Corolario.** *Todo par de curvas se cortan en al menos un punto.*

**Proposición 1.2.3** *(i) Toda curva plana proyectiva lisa $C$ es irreducible.*

*(ii) Toda curva plana proyectiva irreducible $C$ de grado $d$ tiene a lo más $d\cdot(d-1)$ puntos singulares.*

*Demostración*:

(i) Sea $C = \{[x,y,z] \in \mathbb{P}^2 : F(x,y,z)\}$, y supongamos que $C$ es reducible, digamos

$$F(x,y,z) = G(x,y,z)\cdot H(x,y,z),$$

con $G$ y $H$ polinomios homogéneos de grado $> 0$. Por el corolario anterior, $\exists P = [x_0,y_0,z_0]$ perteneciente a la intersección de las curvas definidas por $H(x,y,z)$ y por $G(x,y,z)$, es decir,

$$H(x_0,y_0,z_0) = 0 = G(x_0,y_0,z_0).$$

Ahora $P$ es un punto singular de $C$, ya que

$$\begin{cases} \dfrac{\partial F}{\partial x}(P) &= \dfrac{\partial H}{\partial x}(P)\cdot G(P) + H(P)\cdot\dfrac{\partial G}{\partial x}(P) &= 0 \\ \dfrac{\partial F}{\partial y}(P) &= \dfrac{\partial H}{\partial y}(P)\cdot G(P) + H(P)\cdot\dfrac{\partial G}{\partial y}(P) &= 0 \\ \dfrac{\partial F}{\partial z}(P) &= \dfrac{\partial H}{\partial z}(P)\cdot G(P) + H(P)\cdot\dfrac{\partial G}{\partial z}(P) &= 0. \end{cases}$$

Luego $C$ no puede ser lisa.

(ii) Sea $C = \{[x,y,z] \in \mathbb{P}^2 : F(x,y,z) = 0\}$ una curva proyectiva definida por un polinomio $F(x,y,z)$ homogéneo de grado $d > 0$. Sin pérdida de generalidad podemos suponer que $[0,0,1] \notin C$. En tal caso se tiene que el coeficiente de $z^d$ es distinto de 0. Por lo tanto,

$$F_z(x,y,z) := \frac{\partial F}{\partial z}(x,y,z)$$

es un polinomio homogéneo de grado $d-1$ que no es idénticamente cero. Sea

$$D = \{[x,y,z] \in \mathbb{P}^2 : F_z(x,y,z) = 0\}$$

la curva proyectiva plana definida por $F_z$. Como $C$ es irreducible y de grado $d$, y $D$ es de grado $d-1$, no tienen componentes comunes. Aplicando el Teorema de Bézout a $C$ y $D$ tenemos que a lo más se tienen $d\cdot(d-1)$ puntos de intersección de $C$ y $D$. Ahora bien, como todo punto singular de $C$ es un punto perteneciente a $C \cap D$, tenemos el resultado deseado.

□

## 1.3 Puntos de inflexión.

Damos a continuación dos definiciones de punto de inflexión, una geométrica y otra algebraica. Veremos que son equivalentes.

**Definición.** *Sea $C$ una curva proyectiva plana, $P \in C$ un punto no singular y $L$ la recta tangente a $C$ en $P$. Diremos que $P$ es un* **punto de inflexión de C** *si*

$$I_P(L, C) \geq 3.$$

Para la definición algebraica usaremos el concepto de **hessiano de un polinomio $F(x, y, z)$ en un punto $P$**, que se define como el determinante

$$H_F(P) = \begin{vmatrix} \frac{\partial^2 F}{\partial x^2}(P) & \frac{\partial^2 F}{\partial x \partial y}(P) & \frac{\partial^2 F}{\partial x \partial z}(P) \\ \frac{\partial^2 F}{\partial y \partial x}(P) & \frac{\partial^2 F}{\partial y^2}(P) & \frac{\partial^2 F}{\partial y \partial z}(P) \\ \frac{\partial^2 F}{\partial z \partial x}(P) & \frac{\partial^2 F}{\partial z \partial y}(P) & \frac{\partial^2 F}{\partial z^2}(P) \end{vmatrix}.$$

**Definición.** *Un punto no singular $P$ de una curva proyectiva plana $C$, definida por un polinomio homogéneo $F(x, y, z)$ de grado $d > 0$, se dice que es un* **punto de inflexión de C** *si*

$$H_F(P) = 0.$$

**Ejemplo 1.3.1** Sea $C$ una curva proyectiva plana de grado d.

$$\text{Si } d = 1 \Longrightarrow \text{Todos los puntos de } C \text{ son de inflexión.}$$

Vamos a demostrar que esta afirmación es cierta en ambas definiciones:

(i) Se tiene que la recta tangente $L$ a $C$ en cualquier punto $P$ de $C$ es la misma curva $C$. Por lo tanto:

$$I_P(L, C) = \infty \geq 3.$$

Con lo que todo punto de $C$ es de inflexión.

(ii) Ahora utilizamos la segunda definición de punto de inflexión. Por ser $F(x, y, z)$ de grado 1 tenemos que

$$\frac{\partial^2 F}{\partial x_i \partial x_j}(P) = 0 \quad \forall P \quad x_i, x_j \in \{x, y, z\}.$$

Entonces $H_F(P) = 0 \ \forall P \in C$, y por lo tanto, todo punto de $C$ es punto de inflexión.

De hecho se tiene el siguiente resultado:

**Lema 1.3.1** *Sea* $C = \{[x, y, z] \in \mathbb{P}^2 : F(x, y, z) = 0\}$ *una curva proyectiva irreducible de grado* $d$*. Entonces,*

$$\textit{todos los puntos de } C \textit{ son de inflexión} \iff d = 1.$$

*Demostración*: Ver [KIR], Lema 3.32.

**Lema 1.3.2** *Sea* $C = \{[x, y, z] \in \mathbb{P}^2 : F(x, y, z) = 0\}$ *una curva proyectiva irreducible de grado* 2*. Entonces* $C$ *no tiene puntos de inflexión.*

*Demostración*: Vamos a verlo con las dos definiciones.

(i) Por el Teorema de Bézout, dada cualquier recta $L$ en $\mathbb{P}^2$, tenemos que

$$I_P(C, L) \leq 2 \quad \forall P \in C \cap L.$$

Y en particular para las rectas tangentes a $C$ en cualquier punto $P$ de $C$. Por lo tanto no hay ningún punto de inflexión en la curva $C$.

(ii) Ahora utilizamos la segunda definición de punto de inflexión. $F(x, y, z)$ es un polinomio homogéneo de grado 2, por lo que es de la forma

$$F(x, y, z) = ax^2 + 2bxy + 2cxz + dy^2 + 2eyz + fz^2.$$

El polinomio homogéneo $F$ tiene asociada una forma cuadrática que tiene como matriz

$$A = \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix}.$$

Por ser $C$ irreducible, tenemos que la forma cuadrática asociada es no degenerada (para ver una demostración de esta afirmación ver [HER], Capítulo 13) y por lo tanto

$$det(A) \neq 0.$$

Por otra parte,

$$H_F(P) = det(A) \quad \forall P \in C.$$

Por lo tanto,

$$H_F(P) \neq 0 \quad \forall P \in C;$$

esto es, $C$ no tiene puntos de inflexión.

□

Si $C$ es una curva proyectiva dada por un polinomio homogéneo $F(x, y, z)$, hemos visto que si el grado de $F$ es 1 entonces todos los puntos de $C$ son de inflexión, y si es 2 entonces $C$ no tiene puntos de inflexión. Por lo tanto para $d = 1$ y $d = 2$ los puntos de inflexión obtenidos por ambas definiciones coinciden. Veamos ahora que ambas definiciones de punto de inflexión son equivalentes:

**Proposición 1.3.3** *Sea* $C = \{[x, y, z] \in \mathbb{P}^2 : F(x, y, z) = 0\}$ *una curva proyectiva lisa de grado* $d \geq 3$. *Entonces las dos definiciones de punto de inflexión son equivalentes.*

Antes de la demostración haremos algunas observaciones.

**Observación 1.3.4** (i) Si $F(x, y, z)$ es un polinomio homogéneo de grado $d \geq 2$ entonces los términos de la matriz del hessiano de $F$ son homogéneos de grado $d - 2$. Por lo que $H_F(x, y, z)$ es un polinomio de grado $3 \cdot (d - 2)$.

(ii) El ser un punto de inflexión es independiente de la elección del sistema de coordenadas de $\mathbb{P}^2$.

Ahora sí vamos con la demostración de la proposición.

*Demostración*: Elijamos un sistema de coordenadas proyectivas tal que $P$ sea el origen y la recta tangente a $C$ en $P$ sea el eje $x$. La ecuación afín de la curva en este sistema de coordenadas será

$$F(x, y, 1) = f(x, y) = y + f_2(x, y) + \ldots + f_d(x, y),$$

donde $f_i(x, y) \quad i = 2, \ldots, d$, son polinomios homogéneos de grado $i$. En particular,

$$f_2(x, y) = \alpha x^2 + 2\beta xy + \gamma y^2.$$

Por la primera definición,

$$P \text{ es punto de inflexión} \iff \alpha = 0.$$

Por otra parte, la ecuación proyectiva de $C$ en el correspondiente sistema de coordenadas proyectivas es

$$F(x, y, z) = z^{d-1}y + z^{d-2} \cdot f_2(x, y) + \ldots + f_d(x, y) = 0.$$

Y el hessiano de $F$ en $P = [0, 0, 1]$ es

$$H_F(0, 0, 1) = \begin{vmatrix} 2\alpha & 2\beta & 0 \\ 2\beta & 2\gamma & d-1 \\ 0 & d-1 & 0 \end{vmatrix} = -2(d-1)^2\alpha.$$

Ahora, por la segunda definición,

$$P \text{ es punto de inflexión} \iff F(P) = H_F(P) = 0 \iff \alpha = 0.$$

Con lo que hemos visto que ambas definiciones son equivalentes.

□

Ahora vamos a ver un resultado que nos va decir cuántos puntos de inflexión posee una curva plana proyectiva lisa.

**Proposición 1.3.5** *Sea $C$ una curva plana proyectiva lisa de grado $d \geq 2$. Entonces $C$ tiene exactamente $3d(d-2)$ puntos de inflexión, contando multiplicidades.*

*Demostración*: Por el lema 1.3.2, el caso $d = 2$ está demostrado. Para $d \geq 3$, por la observación 1.3.4, $H_F(x, y, z)$ es un polinomio homogéneo de grado $3(d-2) \geq 0$, ya que $d \geq 3$. Así $H_F$ define la siguiente curva

$$D = \{[x, y, z] \in \mathbb{P}^2 : H_F(x, y, z) = 0\}.$$

Puesto que $C$ es lisa aplicando la Proposición 1.2.3 tenemos que es irreducible.

Además $C$ y $D$ no tienen componentes comunes. Si no fuera así, si $C$ y $D$ tuvieran componentes comunes, $F$ y $H_F$ tendrían factores comunes, de donde todo punto de $C$ sería de inflexión. Pero esto no puede ser, ya que el Lema 1.3.1 nos dice que entonces sería $d = 1$, en contradicción con la hipótesis de que $d \geq 2$. Aplicando ahora el Teorema de Bézout tenemos que

$$\sum_{P \in C \cap D} I_P(C, D) = (\text{grado } C)(\text{grado } D) = 3d(d-2).$$

Por lo tanto, el número de puntos de inflexión, contando multiplicidades, es igual a $3d(d-2)$.

□

## 1.4 Forma de Weierstrass de cúbicas irreducibles.

En esta sección $K$ es un cuerpo, no necesariamente algebraicamente cerrado, y $\overline{K}$ una clausura algebraica fija.

A partir de ahora, diremos que $C$ es una **curva plana definida sobre** $K$ si es una curva proyectiva plana e irreducible sobre $\overline{K}$, dada por un polinomio homogéneo $F(x, y, z) \in K[x, y, z]$.

Los elementos $P \in C(K)$ se llaman **puntos racionales de** $C$ **sobre** $K$.

Si tenemos una curva plana $C$ definida sobre $K$ de grado 3, en determinadas condiciones veremos que podremos escribir $C$ como una curva proyectiva con un único punto en el infinito. Mas aún, podremos encontrar un isomorfismo definido sobre $K$ de tal forma que nuestra curva $C$ será isomorfa a otra con ecuación de la forma

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

con $a_1, a_2, a_3, a_4, a_6 \in K$. Así, el único punto en el infinito será el $[0, 1, 0]$. A esta ecuación se le llama **forma de Weierstrass** de la curva cúbica $C$ dada.

### 1.4.1 Algoritmo de Weierstrass.

En este apartado conseguiremos un algoritmo para poner en determinadas condiciones una curva cúbica en su forma de Weierstrass.

Vamos a ver cúales son estas condiciones. Se distinguen dos casos:

**1**.*Curva cúbica $C$ y $P \in C(K)$ punto de inflexión.*

Se consigue mediante un automorfismo del plano, mandando $P$ al punto $[0,1,0]$ y la recta tangente en $P$ a la recta del infinito, esto es $z=0$. Comprobémoslo:

Supongamos que $C$ está dada por $F=0$ con $F \in K[x,y,z]$ homogéneo de grado 3, digamos

$$F(x,y,z) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + kyz^2 + lz^3,$$

con $a,b,c,d,e,f,g,h,k,l \in K$.

Sea $L$ la recta tangente a $P \in C(K)$, punto de inflexión de $C$. Hacemos el siguiente cambio:

$$\begin{cases} P & \longmapsto & [0,1,0] \\ L & \longmapsto & z=0 \end{cases}$$

Hemos transformado linealmente el polinomio $F(x,y,z)$ a $F_1(x,y,z)$. Tenemos así:

$$F_1(x,y,z) = a'x^3 + b'x^2y + c'xy^2 + d'y^3 + e'x^2z + f'xyz + g'y^2z + h'xz^2 + k'yz^2 + l'z^3,$$

con $a',b',c',d',e',f',g',h',k',l' \in K$.

Vamos a ver qué han de cumplir los coeficientes de $F_1(x,y,z)$:

1. $[0,1,0] \in C = \{[x,y,z] \in \mathbb{P}^2 : F_1(x,y,z)=0\} \Longrightarrow \boxed{d'=0}$
2. La recta tangente en $[0,1,0]$ a $C$ es

$$\frac{\partial F_1}{\partial x}(0,1,0)\cdot x + \frac{\partial F_1}{\partial y}(0,1,0)\cdot y + \frac{\partial F_1}{\partial z}(0,1,0)\cdot z = 0.$$

   Es decir,

$$c'x + 3d'y + g'z = 0.$$

   Sabemos que la recta tangente a $C$ en $[0,1,0]$ es $z=0$. Usando que $d'=0$, se tiene

$$\boxed{c'=0} \quad y \quad \boxed{g' \neq 0}$$

3. Tenemos que $[0,1,0]$ es un punto de inflexión de $C$, por lo tanto,

$$H_{F_1}(0,1,0) = 0.$$

Es decir,

$$\begin{vmatrix} 2b' & 2c' & f' \\ 2c' & 6d' & 2g' \\ f' & 2g' & 2k' \end{vmatrix} = 24b'd'k' + 8c'g'f' - 6f'^2d' + 8g'^2b' + 8k'c'^2 = 0.$$

Usando 1 y 2 obtenemos que

$$\boxed{b' = 0}$$

Ahora utilizando lo anterior tenemos que como $g' \neq 0$ podemos dividir por $g'$, teniendo la misma curva, pero ahora dada por el polinomio:

$$F_2(x, y, z) = Ax^3 + Ex^2z + Gxyz + y^2z + Hxz^2 + Lyz^2 + Mz^3$$

con $A, E, G, H, L, M \in K$. Además se tiene que $A \neq 0$, ya que de lo contrario podriamos escribir

$$F_2(x, y, z) = z \cdot G(x, y, z)$$

con $G(x, y, z) \in K[x, y, z]$ homogéneo de grado 2. Pero esto contradiría la hipótesis de que $C$ era irreducible.

Hagamos ahora el siguiente cambio:

$$\begin{cases} x & \longmapsto & Ax \\ y & \longmapsto & A^2y \\ z & \longmapsto & z. \end{cases}$$

Así obtenemos

$$F_3(x, y, z) = A^4x^3 + EA^2x^2z + GA^3xyz + A^4y^2z + HAxz^2 + LA^2yz^2 + Mz^3.$$

Si finalmente dividimos por $A^4$ y cambiamos el nombre de los coeficientes obtenemos que nuestra curva es

$$C = \{[x, y, z] \in \mathbb{P}^2 : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \ a_i \in K\},$$

como queríamos.

**2**.*Curva cúbica $C$ y $P \in C(K)$ punto no singular y no de inflexión.*

En este caso, si $car(K) \neq 2$, podemos utilizar un argumento algo más complicado, ideado por Nagell ([NAG1]), para reducir a una ecuación de Weierstrass de la forma

$$zy^2 = x^3 + ax^2z + bxz^2 + cz^3 \quad \text{con } a, b, c \in K,$$

que se denomina **forma normal de Weierstrass**.

**Lema 1.4.1** *Sea $C$ una cúbica definida sobre $K$, y sean $P, Q \in C(K)$. Sea $L$ la recta que une $P$ y $Q$. Entonces el tercer punto de corte de $C$ con $L$ (contando multiplicidades) es tambien racional.*

*Demostración*: Supongamos que $C$ está dada por un polinomio homogéneo $F \in K[x,y,z]$. Se tiene que la recta $L$ que une a $P$ con $Q$ está definida sobre $K$, y podemos suponer que su parte afín esta dada por $y = mx + n$ con $m, n \in K$. Los puntos $C(K) \cap L$ cumplen $F(x, mx+n, 1) = f(x, mx+n) = 0$, si tenemos $P = (x_P, y_P), Q = (x_Q, y_Q) \in C(K) \cap L$ entonces $f(x, mx+n) = c(x-x_P)(x-x_Q)(x-x_R)$ y por lo tanto el punto $(x_R, x_R m + n) \in C(K) \cap L$ ya que $f(x, mx+n) \in K[x]$.

□

Sea $L$ la recta tangente a $C$ en $P$; como $P$ no es un punto de inflexión se tiene que $I_P(L, C) = 2$. Además, por el Teorema de Bézout, debe existir un punto $Q \neq P$ tal que $Q \in C(\overline{K}) \cap L$. Por el Lema 1.4.1, tenemos que $Q \in C(K)$.

Ahora, hacemos cambios de coordenadas lineales de tal forma que

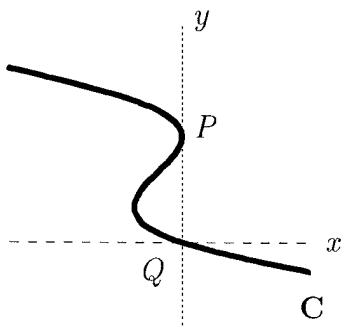
$$\begin{cases} Q & \longmapsto & [0,0,1] \\ L & \longmapsto & x = 0. \end{cases}$$

De esta forma $P$ será un punto en la recta $x = 0$, distinto de $[0,1,0]$ ya que si no $C$ sería reducible. Además, el coeficiente de $z^3$ es 0.

Al tomar la parte afín de $C$, es decir,

$$C' = \{(x,y) \in K^2 : F(x,y,1) = 0\},$$

estamos en la situación siguiente




La curva $C'$ viene dada por $f(x,y) = F(x,y,1) = 0$, donde

$$f(x,y) = f_1(x,y) + f_2(x,y) + f_3(x,y),$$

con $f_i(x,y)$ polinomios homogéneos de grado i.

El eje $y$ corta a la curva $C'$ en $P = (0, y_0)$ para algún $y_0 \in K$, y en $(0,0)$. Además $y_0 \neq 0$ ya que $P$ no era punto de inflexión de $C$ y por lo tanto tampoco $(0, y_0)$ lo es de $C'$. Busquemos los puntos de $C' \cap \{x = 0\}$:

$$\begin{aligned} 0 = f(0,y) &= f_1(0,y) + f_2(0,y) + f_3(0,y) = \\ &= y \cdot f_1(0,1) + y^2 \cdot f_2(0,1) + y^3 \cdot f_3(0,1) = \\ &= y \cdot [f_1(0,1) + y \cdot f_2(0,1) + y^2 \cdot f_3(0,1)]. \end{aligned} \tag{1.1}$$

Por otra parte, sabemos que $C' \cap \{x = 0\} = \{P, Q\}$ con $Q$ simple y $P$ doble (por ser $\{x = 0\}$ la tangente a $C'$ en $P$). El punto $Q = (0, 0)$ corresponde a la solución $y = 0$ en la ecuación (1.1). El punto doble $P = (0, y_0)$ es raíz doble de la ecuación cuadrática

$$f_1(0, 1) + y \cdot f_2(0, 1) + y^2 \cdot f_3(0, 1) = 0.$$

Tenemos así que el discriminante es 0, esto es,

$$[f_2(0, 1)]^2 - 4f_1(0, 1)f_3(0, 1) = 0. \tag{1.2}$$

Ahora si consideramos el corte de la recta $y = tx$ con $C'$, obtenemos

$$\begin{array}{rcccccc} 0 = f(x, tx) & = & f_1(x, tx) & + & f_2(x, tx) & + & f_3(x, tx) = \\ & = & x \cdot f_1(1, t) & + & x^2 \cdot f_2(1, t) & + & x^3 \cdot f_3(1, t) = \\ & = & x \cdot [f_1(1, t) & + & x \cdot f_2(1, t) & + & x^2 \cdot f_3(1, t)]. \end{array}$$

Descartando el caso $x = 0$, obtenemos:

$$x = \frac{-f_2(1, t) \pm \sqrt{[f_2(1, t)]^2 - 4f_1(1, t)f_3(1, t)}}{2f_3(1, t)}.$$

Si hacemos el cambio

$$s = 2f_3(1, t)x + f_2(1, t),$$

obtenemos

$$s^2 = [f_2(1, t)]^2 - 4f_1(1, t)f_3(1, t) = G(t).$$

En principio el grado de $G(t)$ es 4, pero vamos a ver que realmente es 3. Para ello, primero veamos que el coeficiente de $t^4$ es 0.

Sea $f(x, y) = f_3(x, y) + f_2(x, y) + f_1(x, y)$ con $f_i(x, y)$ polinomios homogéneos de grado i, es decir,

$$\begin{aligned} f_3(x, y) &= ax^3 + bxy^2 + cx^2y + dy^3, \\ f_2(x, y) &= ex^2 + fxy + gy^2, \\ f_1(x, y) &= hx + ky. \end{aligned}$$

Entonces,

$$\begin{aligned} f_3(1, t) &= a + bt^2 + ct + dt^3, \\ f_2(1, t) &= e + ft + gt^2, \\ f_1(1, t) &= h + kt. \end{aligned}$$

El coeficiente de $t^4$ en $G(t)$ es

$$g^2 - 4kd.$$

Obsérvese que es identicamente igual a (1.2), por lo que

$$g^2 - 4kd = [f_2(0, 1)]^2 - 4f_1(0, 1)f_3(0, 1) = 0.$$

Y con esto hemos visto que el coeficiente de $t^4$ es 0. Ahora hemos de ver que el coeficiente de grado 3 es distinto de 0. Tenemos la curva afín dada por

$$f(x, y) = ax^3 + bxy^2 + cx^2y + dy^3 + ex^2 + fxy + gy^2 + hx + ky + l.$$

(i) El punto $(0,0)$ pertenece a $C$, por lo tanto $f(0,0)=0$, es decir,

$$\boxed{l=0}$$

como ya sabíamos.

(ii) El punto $(0,y_0)$ es no singular. Además podemos suponer sin pérdida de generalidad que

$$\boxed{y_0=-1},$$

haciendo un simple cambio lineal de coordenadas.

(iii) El punto $(0,0)$ es simple, por lo que se tiene

$$f(0,y)=dy^3+gy^2+ky=y\cdot(dy^2+gy+k),$$

y en consecuencia $\boxed{k\neq 0}$. Ya que de lo contrario tendríamos

$$f(0,y)=y^2\cdot(dy+g)$$

y $(0,0)$ sería un punto doble, en contra de las hipótesis. Por ser $k\neq 0$, podemos dividir por $d$ sin variar la curva. O lo que es lo mismo, tomar $\boxed{k=1}$.

(iv) Tenemos $(0,-1)\in C$. Es decir,

$$0=f(0,-1)=-d+g-k\Longrightarrow \boxed{g=k+d}$$

(v) Además tenemos la condición

$$g^2-4kd=0.$$

Juntando las condiciones (iv) y (v), obtenemos la condición

$$(k-d)^2=0.$$

Por lo tanto $k=d$. Por la condición $(iv)$ obtenemos $g=2k$. Y uniéndolo con el hecho de que $k=1$

$$\boxed{\begin{array}{ccccc} k & = & 1 & = & d \\ & & y & & \\ & g & = & 2 & \end{array}} \tag{1.3}$$

Ahora, el término de $t^3$ en $G(t)$ es

$$2fg-4(hd+kb).$$

Queremos ver que es distinto de 0. Y para comprobarlo, supongamos lo contrario, es decir, que $2fg-4(hd+kb)=0$. Uniendo esto con (1.3), deducimos

$$f=h+b. \tag{1.4}$$

Tenemos

$$\begin{cases} \dfrac{\partial f}{\partial x}(x,y) = 3ax^2 + by^2 + 2cxy + 2ex + fy + h \\ \dfrac{\partial f}{\partial y}(x,y) = 2bxy + cx^2 + 3dy^2 + fx + 2gy + k. \end{cases}$$

Si imponemos las condiciones (1.3) y (1.4) en el sistema, y lo evaluamos en el punto no singular $(0,-1)$ conseguimos

$$\begin{cases} \dfrac{\partial f}{\partial x}(0,-1) = 0 \\ \dfrac{\partial f}{\partial y}(0,-1) = 0 \end{cases}$$

lo cual contradice la hipótesis de que el punto $(0,-1)$ es no singular. Por lo tanto el coeficiente de grado 3 en $G(t)$ es distinto de 0.

□

Hemos obtenido que

$$s^2 = at^3 + bt^2 + ct + d.$$

Y haciendo el cambio

$$\begin{cases} s = a^2 y \\ t = ax, \end{cases}$$

la curva $C$ viene dada por

$$y^2 = x^3 + Ax^2 + Bx + C.$$

Ahora homogeneizando, es decir, haciendo el cambio

$$\begin{cases} y = \frac{Y}{Z}, \\ x = \frac{X}{Z}, \end{cases}$$

tenemos nuestra curva dada por la forma de Weierstrass

$$Y^2Z = X^3 + AX^2Z + BXZ^2 + CZ^3.$$

### 1.4.2 Condiciones necesarias y suficientes para aplicar el algoritmo de Weierstrass.

Tenemos una curva $C$ proyectiva plana irreducible definida por un polinomio homogéneo de grado 3 sobre $K$. Ahora nos preguntamos:
¿Cuándo puedo encontrar un isomorfismo, definido sobre $K$, de tal forma que $C \cong \{[x,y,z] \in \mathbb{P}^2 : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \ a_i \in K\}$?

Una condición necesaria y suficiente para poder encontrar dicho isomorfismo es que

$$C(K) \neq \emptyset.$$

El algoritmo de Weierstrass nos muestra que la condición es suficiente ya que:

(i) Si $P \in C(K)$ es un punto de inflexión podemos aplicar **1** del algoritmo.

(ii) Si $P$ no es de inflexión y es no singular aplicamos **2**.

(iii) Si $P$ es singular entonces es un punto doble (como veremos en la sección §1.1.5). Por el Teorema de Bézout existe $Q \in C(\overline{K})$ (corte de cualquier recta que pase por $P$ con $C$) no singular. Además, por el Lema 1.4.1, $Q \in C(K)$ y entonces aplicamos el algoritmo a $Q$.

Distinguiremos dos casos, cuando $K$ es algebraicamente cerrado y cuando no lo es.

**1.** *$K$ algebraicamente cerrado.*

Se tiene el siguiente hecho importante:

$$K = \overline{K} \Longrightarrow \#C(K) = \infty.$$

Por ser $C$ una curva irreducible el número de puntos singulares es finito, por la Proposición 1.2.3. Entonces podemos coger un punto no singular de $C(K)$ y aplicar el apartado **2** del algoritmo de Weierstrass para así conseguir poner $C$ en su forma de Weierstrass.

En particular si $C$ es no singular, $C$ tiene un punto de inflexión, por la Proposición 1.3.5. Entonces en este caso también podemos aplicar el apartado **1** del algoritmo de Weierstrass para conseguir poner $C$ en su forma de Weierstrass.

En definitiva, *si $K$ es algebraicamente cerrado, siempre podemos encontrar una ecuación de Weierstrass para $C$.*

**2.** *$K$ no algebraicamente cerrado.*

En este caso no siempre vamos a poder poner la curva $C$ en su forma de Weierstrass. Por ejemplo si $K = \mathbb{Q}$, que es el caso que más nos interesa, Selmer dió el siguiente ejemplo:

$$C(\mathbb{Q}) = \{[x, y, z] \in \mathbb{P}^2(\mathbb{Q}) : 3x^3 + 4y^3 + 5z^3 = 0\}$$

y demostró que $\#C(\mathbb{Q}) = \emptyset$. Para ver la demostración de este hecho ver [SEL] o [CAS], Capítulo 18. En este caso no podemos aplicar el algoritmo de Weierstrass.

De hecho es claro que no podemos ponerlo en la forma de Weierstrass, ya que no tiene ningún punto y la forma de Weierstrass siempre tiene el punto $[0, 1, 0]$.

## 1.5 Curvas en forma de Weierstrass.

En esta sección supondremos que ya tenemos una curva $C$ dada por una ecuación de Weierstrass. Como hemos visto en la sección §1.4.2 basta con que $C(K) \neq \emptyset$.

Consideremos una curva de la forma

$$C = \{[x, y, z] \in \mathbb{P}^2 : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\}.$$

Diremos que $C$ está **definida sobre** $K$ si $a_1, a_2, a_3, a_4, a_6 \in K$ y lo denotaremos por $C/K$. Así, $\mathcal{O} = [0, 1, 0] \in C$ es un punto de inflexión de $C$. Si tomamos coordenadas no homogéneas

$$\begin{cases} x = \frac{X}{Z}, \\ \\ y = \frac{Y}{Z}, \end{cases}$$

obtenemos la curva afín dada por

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.5}$$

Podemos reducir aún esta ecuación:

- Si $car(\overline{K}) \neq 2$, hacemos el siguiente cambio

  $$\begin{cases} x & \longmapsto & x \\ y & \longmapsto & \frac{1}{2}(y - a_1x - a_3), \end{cases}$$

  y conseguimos describir la curva con la ecuación

  $$\boxed{y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6} \tag{1.6}$$

  donde

  $$\begin{cases} b_2 = a_1^2 + 4a_2, \\ b_4 = 2a_4 + a_1a_3, \\ b_6 = a_3^2 + 4a_6. \end{cases} \tag{1.7}$$

- Si $car(\overline{K}) \neq 2, 3$. En la ecuación (1.6), hacemos el cambio

  $$\begin{cases} x & \longmapsto & \dfrac{x - 3b_2}{36}, \\ \\ y & \longmapsto & \dfrac{y}{216}, \end{cases}$$

  obteniendo la ecuación

  $$\boxed{y^2 = 4x^3 - 27c_4x - 54c_6}, \tag{1.8}$$

  con

  $$\begin{cases} c_4 = b_2^2 - 24b_4, \\ c_6 = b_2^3 + 36b_2b_4 - 216b_6. \end{cases} \tag{1.9}$$

Y podemos hacer un cambio para dejar más simplificada aún la ecuación,

$$\begin{cases} x \longmapsto 4x, \\ y \longmapsto 4^2 x, \end{cases}$$

y así tenemos que $C$ esta dada por la ecuación

$$\boxed{y^2 = x^3 + Ax + B} \tag{1.10}$$

con

$$\begin{cases} A = -\dfrac{27}{4^3} c_4, \\ B = -\dfrac{27}{4^3 \cdot 2} c_6. \end{cases} \tag{1.11}$$

**Nota**: A partir de ahora $car(\overline{K}) \neq 2, 3$.

**Observación 1.5.1** Si tenemos una curva $C$ definida sobre $\mathbb{R}$, en particular sobre $\mathbb{Q}$, dada por una ecuación de Weierstrass, podemos ver gráficamente cómo va a ser la parte real de $C$.

Si

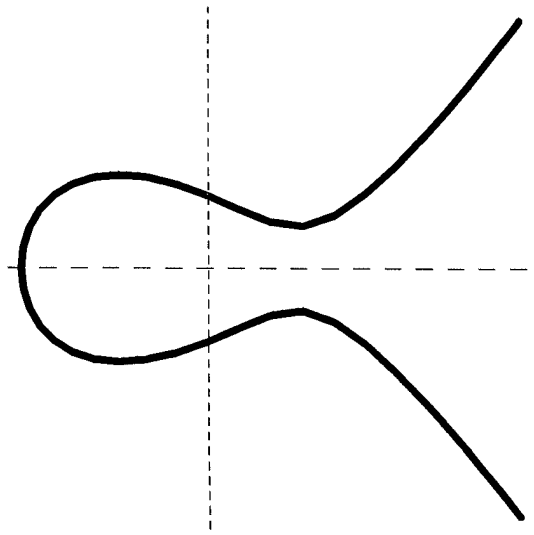
$$C' = \{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + Ax + B\},$$

va a haber cuatro tipos de gráficas de $C'$, dependiendo de cómo son las raíces de $f(x) = x^3 + Ax + B$. Si escribimos

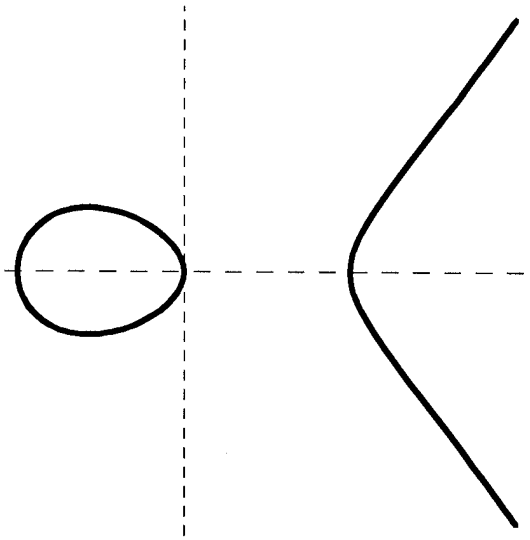
$$f(x) = (x - \alpha)(x - \beta)(x - \gamma),$$

se va a tener la situación siguiente

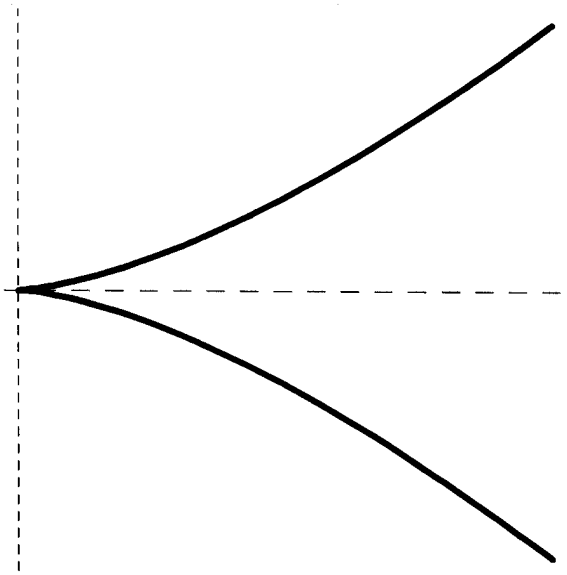
1. Si $\alpha \in \mathbb{R}$ y $\beta, \gamma \notin \mathbb{R}$, entonces $C'$ es gráficamente de la forma:



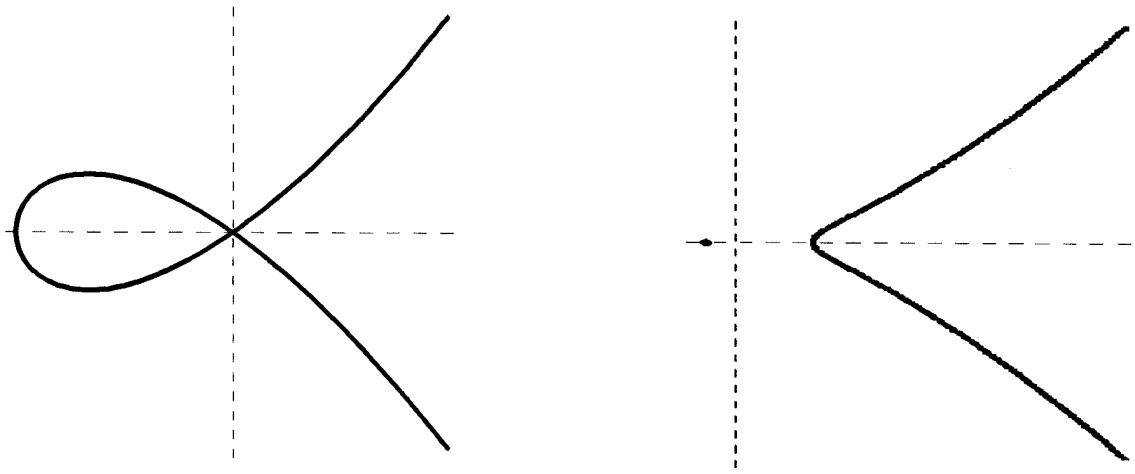
2. Si $\alpha, \beta, \gamma \in \mathbb{R}$ distintas.



3. $\alpha = \beta = \gamma \in \mathbb{R}$.



4. $\alpha, \beta, \gamma \in \mathbb{R}$ $\alpha = \beta \neq \gamma$. Tenemos dos posibilidades dependiendo de si las tangentes al punto singular son reales o complejas.



Veremos que los casos 1 y 2 son el caso de una curva lisa, mientras que los casos 3 y 4 son curvas singulares.

Supongamos que tenemos un punto $P = (x_0, y_0)$ que satisface la ecuación de Weierstrass en su forma afín,

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Asumimos que $P$ es un punto singular de la curva definida por los puntos que satisfacen $f(x, y) = 0$. Por ser punto singular satisface que

$$\begin{cases} \dfrac{\partial f}{\partial x}(x_0, y_0) = 0, \\ \dfrac{\partial f}{\partial y}(x_0, y_0) = 0. \end{cases}$$

Hacemos el desarrollo de Taylor de $f(x, y)$ en $P = (x_0, y_0)$

$$f(x, y) = [(y - y_0) - \alpha(x - x_0)] \cdot [(y - y_0) - \beta(x - x_0)] - (x - x_0)^3 \qquad (1.12)$$

para algunos $\alpha, \beta \in \overline{K}$.

**Definición.** *Sea $P = (x_0, y_0)$ un punto singular de una curva cúbica irreducible afín. Diremos que*

- *$P$ es un* **nodo** *si $\alpha \neq \beta$ en (1.12).*
- *$P$ es una* **cúspide** *si $\alpha = \beta$ en (1.12).*

Es decir tenemos:

- En el caso de un nodo. Hay dos rectas tangentes, que son:

$$\begin{cases} y - y_0 = \alpha(x - x_0), \\ y - y_0 = \beta(x - x_0). \end{cases}$$

- En el caso de una cúspide. Hay una recta tangente doble que es:

$$y - y_0 = \alpha(x - x_0).$$

Ahora veremos que en una curva cúbica irreducible sólo hay, como mucho, un punto singular.

**Proposición 1.5.2** *Sea $C$ una curva cúbica proyectiva irreducible. Entonces $C$ tiene como mucho un punto singular.*

*Demostración*: Supongamos que hay más de un punto singular. Sean $P$ y $Q$ puntos singulares distintos. Consideremos la recta $L$ que pasa por ambos puntos. Por ser $P$ y $Q$ puntos singulares se tiene que

$$I_P(C, L), I_Q(C, L) \geq 2.$$

Como $C$ es irreducible, entonces $C$ y $L$ no tienen componentes comunes. Por lo que podemos aplicar el Teorema de Bézout

$$3 = (grado(C)) \cdot (grado(L)) = \sum_{P' \in C \cap L} I_{P'}(C, L) \geq I_P(C, L) + I_Q(C, L) \geq 4.$$

Por lo tanto como mucho existe un punto singular.

□

**Definición.** *Sea $C = \{[x, y, z] \in \mathbb{P}^2 : y^2z = x^3 + Axz^2 + Bz^3\}$. Definimos:*

- *El* **discriminante de C** *es* $\Delta := -16(4A^3 + 27B^2)$.
- *El* **invariante j de C** *es* $j := 1728\dfrac{(4A)^3}{\Delta}$.

**Observación 1.5.3** Supongamos que tenemos, como al principio del apartado, una curva $C$ definida por una ecuación de Weierstrass,

$$C = \{[x, y, z] \in \mathbb{P}^2 : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\}.$$

Entonces el punto $\mathcal{O} = [0, 1, 0]$, que jugará un importante papel en los apartados siguientes, es un punto no singular de $C$; más aún, es un punto de inflexión de $C$. Con esto tenemos que el único punto en el infinito de $C$ es $\mathcal{O}$. Y escribimos

$$C(K) = \{(x, y) \in \mathbb{A}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}.$$

Comprobemos estas últimas afirmaciones:

- $\mathcal{O}$ es no singular. Es fácil verlo, ya que si definimos

$$F(x,y,z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3,$$

entonces

$$\frac{\partial F}{\partial z}(\mathcal{O}) \neq 0.$$

- $\mathcal{O}$ es punto de inflexión. Se tiene que

$$H_F(P) = \begin{vmatrix} \frac{\partial F}{\partial x^2}(P) & \frac{\partial F}{\partial x\partial y}(P) & \frac{\partial F}{\partial x\partial z}(P) \\ \frac{\partial F}{\partial y\partial x}(P) & \frac{\partial F}{\partial y^2}(P) & \frac{\partial F}{\partial y\partial z}(P) \\ \frac{\partial F}{\partial z\partial x}(P) & \frac{\partial F}{\partial z\partial y}(P) & \frac{\partial F}{\partial z^2}(P) \end{vmatrix} = \begin{vmatrix} 0 & 0 & a_1 \\ 0 & 0 & 2 \\ a_1 & 2 & 2a_3 \end{vmatrix} = 0.$$

También podemos verlo con la otra definición de punto de inflexión. Es decir, viendo que el único punto de corte con la recta tangente es $\mathcal{O}$. La recta tangente a $C$ en $\mathcal{O}$ es $z = 0$. Y tenemos

$$C \cap \{z = 0\} = \{[x,y,z] \in \mathbb{P}^2 : F(x,y,0)\} \Longrightarrow x^3 = 0.$$

Por tanto, el único punto de corte es $\mathcal{O} = [0,1,0]$.

□

Ahora supongamos que nuestra curva es de la forma

$$y^2 = f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

con $\alpha_1, \alpha_2, \alpha_3 \in \overline{K}$. Definimos el **discriminante de** $f$ como

$$d = (\alpha_1 - \alpha_2)^2 \cdot (\alpha_1 - \alpha_3)^2 \cdot (\alpha_2 - \alpha_3)^2.$$

Y si $f(x)$ esta dado en la forma

$$f(x) = x^3 + Ax + B$$

entonces, mediante un sencillo cálculo llegamos a que

$$d = -4A^3 - 27B^2.$$

Por lo tanto, si nuestra curva es

$$C = \{(x,y) \in \mathbb{A}^2 : y^2 = x^3 + Ax + B\} \cap \{\mathcal{O}\},$$

entonces

$$\boxed{\Delta = 2^4 d}. \tag{1.13}$$

Con esto vamos a clasificar nuestras curvas cúbicas irreducibles.

**Teorema 1.5.4** *Sea $C$ una curva cúbica irreducible dada por su ecuación normal de Weierstrass,*

$$C : y^2 = f(x) = x^3 + Ax + B.$$

*Entonces*

$$\begin{aligned} C \text{ es singular} &\iff \Delta = 0. \\ &\iff d = 0. \\ &\iff f \text{ tiene raíces repetidas.} \end{aligned}$$

*Demostración*: Es obvio, por la definición del discriminante, que $d = 0$ es equivalente a que $f(x)$ tenga raíces repetidas. También es obvio que $\Delta = 0 \iff d = 0$, por la relación (1.13). Por lo tanto, sólo nos queda ver que $C$ es singular si y sólo si $d = 0$. Nuestra curva viene dada por

$$C : zy^2 = x^3 + Axz^2 + Bz^3.$$

Pongamos $F(x, y, z) = zy^2 - x^3 - Axz^2 - Bz^3$. Sabemos que el único punto de intersección de $C$ con la recta del infinito, $z = 0$, es $\mathcal{O}$. Y además hemos demostrado que no es singular. Por lo tanto, si un punto $P = [x_0, y_0, z_0] \in C$ es singular se tiene que $z_0 \neq 0$. Así que podemos suponer que $z_0 = 1$. Ahora bien, si un punto $P = [x_0, y_0, 1] \in C$ es singular se ha de tener que

$$\frac{\partial F}{\partial x}(x_0, y_0, 1) = \frac{\partial F}{\partial y}(x_0, y_0, 1) = \frac{\partial F}{\partial z}(x_0, y_0, 1) = 0.$$

Es decir,

$$\begin{cases} -3x_0^2 - A &= 0, \quad (a) \\ 2y_0 &= 0, \quad (b) \\ y_0^2 - 2A - 3B &= 0. \quad (c) \end{cases}$$

La ecuación $(b)$ nos dice que $y_0 = 0$. Ahora vamos a distinguir dos casos, cuando $A \neq 0$ y cuando $A = 0$.

1. $A \neq 0$.
   Entonces por $(c)$ tenemos $x_0 = -\frac{3}{2}\frac{B}{A}$, y sustituyendo esto en $(a)$ obtenemos

   $$\frac{1}{4A^2}(27B^2 + 4A^3) = 0 \iff d = 0.$$

2. $A = 0$.
   Tenemos

   $$\begin{cases} 3x_0 &= 0 \\ 3B &= 0 \end{cases} \iff \begin{cases} x_0 &= 0, \\ B &= 0. \end{cases}$$

   Con lo que llegamos a que esto ocurre si y sólo si $d = 0$.

□

**Observación 1.5.5** Vamos a clasificar las cúbicas definidas sobre $\mathbb{R}$, en particular sobre $\mathbb{Q}$, que tienen una ecuación de Weierstrass de la forma

$$C : y^2 = x^3 + Ax + B.$$

Para ello vamos a utilizar el discriminante de $C$. Van a ocurrir varios casos. Sea

$$f(x) = x^3 + Ax + B$$

y $\Delta$ el discriminante de la curva definida por

$$C = \{(x, y) \in \mathbb{A}^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

1. $\Delta \neq 0 \Longrightarrow C$ es lisa. Se tienen los dos casos siguientes:

   (a) $\Delta < 0 \Longrightarrow$ La ecuación $f(x) = 0$ tiene una sola raíz real, y el grafo real afín de la curva tiene una sóla componente conexa.

   (b) $\Delta > 0 \Longrightarrow$ La ecuación $f(x) = 0$ tiene tres raíces reales distintas, y el grafo real afín de la curva tiene dos componentes conexas: una no compacta, que es la componente de la curva cuyo cierre proyectivo contiene a $\mathcal{O}$, y una compacta, de forma oval.

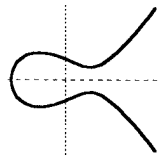
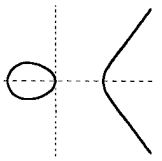
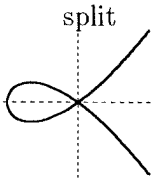
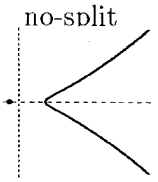
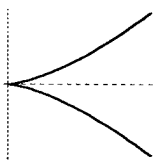
2. $\Delta = 0 \Longrightarrow C$ es singular y contiene un sólo punto singular. Este caso se divide en tres subcasos. Como el polinomio $f(x)$ tiene al menos una raíz doble, escribimos $f(x) = (x-\alpha)^2(x-\beta)$ y como $f(x) = x^3 + Ax + B$ obtenemos que $2\alpha + \beta = 0$, por lo tanto $f(x) = (x - \alpha)^2(x + 2\alpha)$.

   (a) $\alpha > 0 \Longrightarrow$ El grafo real afín tiene una única componente conexa, que posee un punto doble en $x = \alpha$. Las tangentes en el punto doble tiene pendientes reales distintas.

   (b) $\alpha < 0 \Longrightarrow$ El grafo real afín tiene dos componentes conexas: una no compacta, y un punto aislado de coordenadas $(\alpha, 0)$. De hecho este punto es de nuevo un punto doble, pero con tangentes distintas de pendientes complejas.

   (c) $\alpha = 0 \Longrightarrow$ La curva tiene una cúspide en $(0, 0)$, es decir las tangentes en el punto singular $(0, 0)$ son la misma.

A las curvas que cumplen las condiciones de $2(a)$ y $2(b)$ las llamaremos **cúbicas de degeneración multiplicativa** y al caso $2(c)$ **cúbicas de degeneración aditiva**. El porqué de estos nombres se verá claro al ver la proposición 1.6.7. Para diferenciar los casos de degeneración multiplicativa, llamaremos **degeneración multiplicativa split** al caso $2(a)$ y **degeneración multiplicativa no split** al caso $2(b)$. Todo esto se resume en la siguiente tabla:

<table>
<tr><td colspan="2">$C$ lisa</td><td colspan="3">$C$ singular</td></tr>
<tr><td colspan="2">$\Delta \neq 0$</td><td colspan="3">$\Delta = 0$</td></tr>
<tr><td colspan="2">$f(x) = (x-\alpha)(x-\beta)(x-\gamma)$<br>$\alpha \neq \beta \neq \gamma$</td><td colspan="3">$f(x) = (x-\alpha)^2(x+2\alpha)$</td></tr>
<tr><td>$\Delta < 0$<br>$\alpha \in \mathbb{R}, \beta, \gamma \notin \mathbb{R}$</td><td>$\Delta > 0$<br>$\alpha, \beta, \gamma \in \mathbb{R}$</td><td colspan="2">$\alpha \neq 0$<br>Degeneración multiplicativa</td><td>$\alpha = 0$<br>Degeneración aditiva</td></tr>
<tr><td>  </td><td>  </td><td>split<br>  <br>$\alpha > 0$</td><td>no-split<br>  <br>$\alpha < 0$</td><td>  </td></tr>
</table>

El caso de degeneración multiplicativa tambien se conoce con el nombre de **cúbica nodal** y al caso de degeneración aditiva con el de **cúbica cuspidal.**

**Definición.** *Sean $C_1$ y $C_2$ curvas proyectivas planas irreducibles. Una* **aplicación racional entre $C_1$ y $C_2$** *es una aplicación de la forma*

$$\begin{array}{rccc} \phi: & C_1 & \longrightarrow & C_2 \\ \phi = & [f_0, f_1, f_2] & & \end{array}$$

*donde $f_0, f_1, f_2 \in \overline{K}(x,y,z)$ (el cuerpo de fracciones de $\overline{K}[x,y,z]$) tienen la propiedad de que para todo $P \in C_1$ en donde $f_0, f_1, f_2$ estén definidas,*

$$\phi(P) = [f_0(P), f_1(P), f_2(P)] \in C_2.$$

*Si $\exists \lambda \in \overline{K}^*$ tal que $\lambda f_0, \lambda f_1, \lambda f_2 \in K(x,y,z)$ entonces diremos que $\phi$ está* **definida sobre $K$.**

*Diremos que $C_1$ y $C_2$ son* **birracionalmente equivalentes** *si existe una aplicación racional de $C_1$ en $C_2$ con inversa racional.*

Ahora vamos a ver un resultado relacionado con esta última definición que será importante en lo que definiremos como curva elíptica.

**Proposición 1.5.6** *Sea $C$ una curva cúbica proyectiva dada por una forma de Weierstrass. Si $C$ es singular $\Longrightarrow$ $C$ es birracionalmente equivalente a $\mathbb{P}^1$.*

*Demostración*: Sea

$$C = \{[x,y,z] \in \mathbb{P}^2 : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\} = \{(x,y) \in \mathbb{A}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}.$$

y $P = (x_0, y_0)$ el punto singular de $C$. Hacemos el cambio siguiente:

$$\begin{cases} x & \longmapsto & x + x_0, \\ y & \longmapsto & y + y_0. \end{cases}$$

Con él obtenemos que $(0,0)$ es el punto singular. Y la parte afín de $C$ viene dada por

$$y^2 + b_1xy = x^3 + b_2x^2,$$

ya que si $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ obtenemos:

- $(0,0) \in C \Longrightarrow f(0,0) = 0 \Longrightarrow a_6 = 0.$
- $P$ es singular: $\dfrac{\partial f}{\partial x}(0,0) = \dfrac{\partial f}{\partial y}(0,0) = 0 \Longrightarrow b_4 = b_3 = 0.$

Así obtenemos que $C = \{(x,y) \in \mathbb{A}^2 : y^2 + b_1xy = x^3 + b_2x^2\} \cup \{\mathcal{O}\}$. Y podemos construir la siguiente función racional:

$$\begin{array}{rccc} \phi : & C & \longrightarrow & \mathbb{P}^1 \\ & (x,y) & \longmapsto & [x,y] \end{array}$$

con inversa

$$\begin{array}{rccc} \phi^{-1} : & \mathbb{P}^1 & \longrightarrow & C \\ & [1,t] & \longmapsto & (t^2 + b_1t - b_2, t^3 + b_1t^2 - b_2t). \end{array}$$

Por lo tanto $\mathbb{P}^1$ y $C$ son birracionalmente equivalentes.

□

**Definición.** *Una* **curva elíptica** *es una curva proyectiva plana $E$ lisa de grado* 3 *junto con un punto $\mathcal{O} \in E$. Lo denotaremos por $(E, \mathcal{O})$.*

*La curva elíptica $(E, \mathcal{O})$ es* **definida sobre** *$K$, y escribiremos $E/K$, si $E$ está definida sobre $K$ y $\mathcal{O} \in E(K)$. A los puntos $P \in E(K)$ les llamaremos* **puntos racionales sobre** *$K$.*

Con esta definición hemos excluído a las curvas cúbicas singulares. En el capítulo 2 daremos una nueva definición de curva elíptica que será totalmente equivalente a esta definición. En la proposición 1.5.6 vimos que una cúbica singular es birracionalmente equivalente a $\mathbb{P}^1$. Esta será la razón por la que excluímos las curvas cúbicas singulares. Ya que como veremos en el capítulo 2 una curva elíptica es una curva lisa de género[1] 1. Y con esta definición excluimos el caso de curvas birracionalmente equivalentes a $\mathbb{P}^1$, que tienen[2] género 0.

Vamos a utilizar el invariante $j$ para clasificar las curvas elpticas.

[1]Para ver la definición de género ver el capítulo 2.

[2]Ver ejemplo 2.5.4.

**Teorema 1.5.7** *Dos curvas elípticas son isomorfas (sobre $\overline{K}$) si y sólo si tienen el mismo invariante $j$.*

*Demostración:* Supongamos[3] que $car(K) \neq 2, 3$. Sean $C_1$ y $C_2$ las curvas elípticas dadas por

$$C_1 : y^2 = x^3 + Ax + B$$
$$C_2 : (y')^2 = (x')^3 + A'x' + B'.$$

Como veremos en el teorema 2.6.1, el único cambio de variables fijando $[0, 1, 0]$ y preservando la forma de Weierstrass de la ecuación de la curva es de la forma

$$\begin{cases} x = u^2x' + r, \\ y = u^3y' + u^2sx + t, \end{cases}$$

con $u, r, s, t \in \overline{K}, u \neq 0$. Así, si $C_1$ y $C_2$ son isomorfas, una se transforma en la otra mediante un cambio de la forma anterior. Y un sencillo cálculo nos muestra que si denotamos por $j_1$ al invariante $j$ de $C_1$ y $j_2$ al de $C_2$ obtenemos que

$$j_1 = j_2.$$

Supongamos ahora que $j = j_1 = j_2$. Entonces

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4(A')^3 + 27(B')^2},$$

y simplificando obtenemos

$$A^3(B')^2 = (A')^3B^2.$$

Buscamos un isomorfismo de la forma $(x, y) = (u^2x', u^3y')$ y consideramos tres casos:

1. $A = 0$. Entonces $j = 0$ y $B \neq 0$ ya que $\Delta \neq 0$. Obtenemos un isomorfismo usando $u = (B/B')^{1/6}$.

2. $B = 0$. Por tanto $j = 1728$. Entonces $A \neq 0$ ya que $\Delta \neq 0$. Consegimos un isomorfismo usando $u = (A/A')^{1/4}$.

3. $AB \neq 0$. Por lo que $j \neq 0, 1728$. Entonces $A'B' \neq 0$ ya que si uno es cero el otro también y entonces $\Delta = 0$, contradicción. Entonces tomando $u = (A/A')^{1/4} = (B/B')^{1/6}$ obtenemos un isomorfismo.

□

**Teorema 1.5.8**

$$\{\textit{Curvas elípticas definidas sobre } \overline{K}\}/\{\textit{Isomorfismos}\} \cong \overline{K}.$$

[3]Para los casos $car(K) = 2, 3$ ver [SIL], Apéndice A, Proposición 1.2,b.

*Demostración:* Basta con ver que para $j_0 \in \overline{K}$ existe una curva elíptica (definida sobre $K(j_0)$) con invariante $j$ igual a $j_0$, así obtendremos la sobreyectividad. La inyectividad nos la da el teorema anterior.

Supongamos que $j_0 \neq 0, 1728$ y tomemos la curva

$$C : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

Calculando obtenemos:

$$\Delta = \frac{{j_0}^2}{(j_0 - 1728)^3} \quad \text{y} \quad j = j_0.$$

Entonces $C$ es la curva elíptica que buscábamos (en cualquier característica) para $j_0 \neq 0, 1728$. Para completar la lista usamos las curvas

$$\begin{array}{lll} C : y^2 + y = x^3 & \Delta = -27 & j = 0; \\ C : y^2 = x^3 + x & \Delta = -64 & j = 1728. \end{array}$$

Hacemos notar que en característica 2 y 3, 1728 es igual a 0. En ambos casos una de las dos curvas es no singular.

□

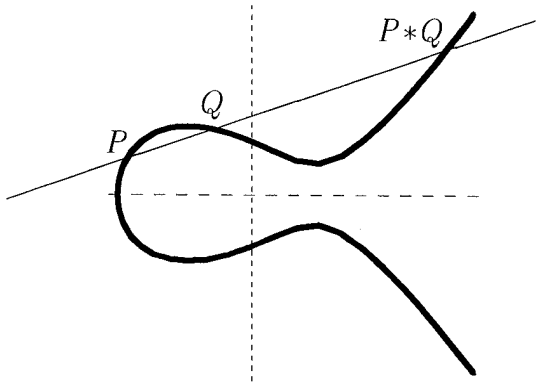
## 1.6 Grupo abeliano asociado a una curva elíptica.

Vamos a dotar a una curva elíptica de una estructura de grupo abeliano.

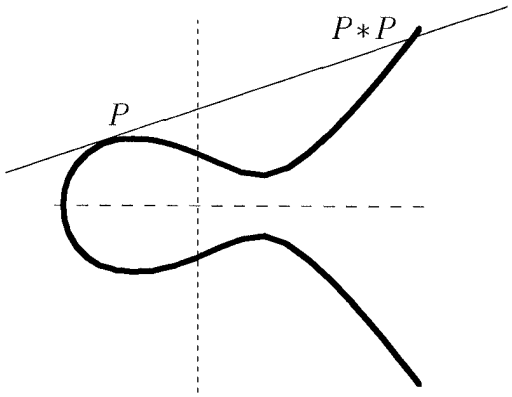
Sea $E$ una curva elíptica definida sobre un cuerpo $K$, con un punto $\mathcal{O} \in E(K)$. Consideramos $P$ y $Q \in E(K)$, y tomemos la recta que los une. Entonces, por el Lema 1.4.1, se tiene que el tercer punto de corte, que denotaremos por $P * Q$, pertenece a $E(K)$. En el caso $P = Q$, tomaremos la recta tangente a $E(K)$ por $P$, y esta recta cortará (de nuevo usando el Teorema de Bézout y utilizando el hecho de que $E$ es lisa) a $E$ en otro[4] punto de $E(K)$, que denotaremos por $P * P$.

Así se obtiene una ley de composición $*$.

[4]En el caso de que $P$ sea un punto de inflexión de $E$, el tercer punto de corte es el mismo $P$.




$P * Q$ con $P \neq Q$




$P * P$

**Observación 1.6.1** Se verifican de forma inmediata las siguientes propiedades de la ley de composición $*$.

(i) $P * Q = Q * P \quad \forall P, Q \in E(K)$.

(ii) $(P * Q) * Q = P \quad \forall P, Q \in E(K)$.

Ahora vamos a considerar todos los puntos racionales de una curva elíptica definida sobre $K$. Y vamos a dar una ley de composición en $E(\mathbf{K})$ para dotarlo de estructura de grupo. Dados cualesquiera dos puntos $P, Q \in E(K)$, tenemos definido un tercer punto $P * Q \in E(K)$. Y ahora nos preguntamos qué estructura algebraica tiene $E(K)$ junto con la ley de composición $*$. Por ejemplo,

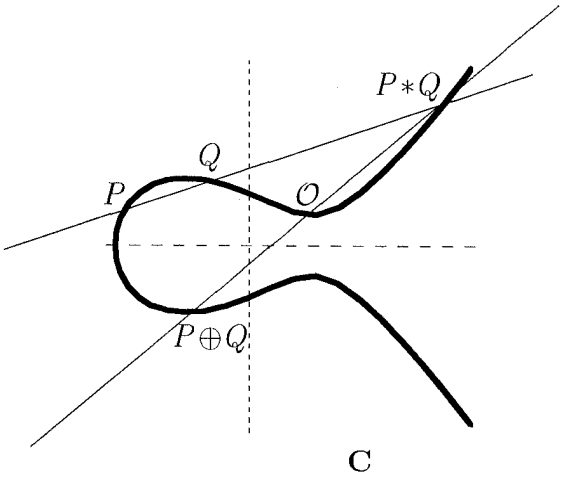
$$\text{¿es } (E(K), *) \text{ un grupo?}$$

Desafortunadamente, no es un grupo en general, ya que no hay un elemento identidad. Pero modificando un poco esta ley de composición, podemos conseguir que $E(K)$ sea un grupo (haremos que $\mathcal{O} \in E(K)$ sea el elemento neutro de nuestra próxima ley de grupo). La ley de grupo, a la que denotaremos por $\oplus$, va a ser:

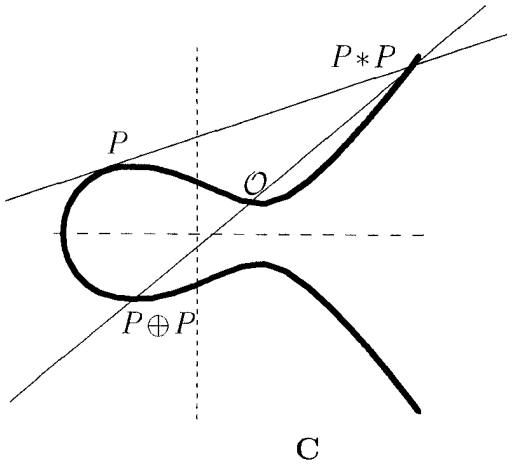
**Ley de grupo**: Sean $P, Q \in E(K)$, $L$ la recta que une $P$,$Q$ (recta tangente en $P$ a $E(K)$ si $P = Q$) y $P * Q$ el tercer punto de intersección de $L$ con $E(K)$. Sea $L'$ la recta que une $P * Q$ con $\mathcal{O}$. Entonces $P \oplus Q$ es el tercer punto de intersección de $L'$ y $E(K)$. Es decir,

$$\boxed{P \oplus Q := \mathcal{O} * (P * Q)}$$

Gráficamente,




$P \oplus Q$ con $P \neq Q$




$P \oplus P$

Antes de estudiar las propiedades de $\oplus$, recordamos el siguiente teorema:

**Teorema 1.6.2** *Sean $P_1, \ldots, P_8$, 8 puntos de $\mathbb{P}^2$ en* **posición general** *(es decir, no hay cuatro de los puntos en una recta y no hay siete de los puntos en una cónica). Entonces existe un noveno punto $Q$ tal que toda cúbica que pase por $P_1, \ldots, P_8$ pasa por $Q$.*

*Demostración*: Una cúbica plana viene dada por

$$C = \{[x, y, z] \in \mathbb{P}^2 : F(x, y, z) = 0\},$$

con $F(x, y, z) \in K[x, y, z]$ homogéneo de grado 3. Es decir $F$ es de la forma

$$F(x, y, z) = a_1x^3+a_2x^2y+a_3x^2z+a_4xy^2+a_5xz^2+a_6y^3+a_7y^2z+a_8yz^2+a_9z^3+a_{10}xyz$$

con $a_1, \dots a_{10} \in K$. Vemos que $F$ tiene 10 coeficientes.

Por estar los 8 puntos en posición general, las condiciones lineales $F(P_i) = 0$, $i = 1, \dots, 8$ sobre los coeficientes de $F$ son independientes. Por tanto las cúbicas planas que pasan por $P_1, \dots, P_8$ forman un espacio vectorial de dimensión 2.

Sean $C_1$ y $C_2$ dos cúbicas independientes tales que $P_1, \dots, P_8 \in C_1 \cap C_2$. Sean $F_1, F_2 \in K[x, y, z]$ los polinomios homogéneos de grado 3 que definen las curvas $C_1$ y $C_2$ respectivamente. Entonces, cualquier cúbica que pase por $P_1, \dots, P_8$ estará definida por un polinomio homogéneo con coeficientes en $K$ de grado 3 de la forma

$$F(x, y, z) = \lambda F_1(x, y, z) + \mu F_2(x, y, z) \quad \lambda, \mu \in K. \tag{1.14}$$

Por el Teorema de Bézout, $C_1$ y $C_2$ tienen 9 puntos en común, por lo que existe un noveno punto $Q \in C_1 \cap C_2$ tal que $Q \neq P_i$, $i = 1 \dots 8$. Por lo tanto toda cúbica definida por (1.14) pasa por el noveno punto $Q$. Y esto demuestra el teorema.

□

Ahora veamos las propiedades de $\oplus$.

**Propiedades de $\oplus$**:

(i) $P \oplus \mathcal{O} = P \quad \forall P \in E(K)$.

(ii) $P \oplus Q = Q \oplus P \quad \forall P, Q \in E(K)$.

(iii) $\forall P \in E(K), \exists P' \in E(K)$ tal que $P \oplus P' = \mathcal{O}$. A $P'$ lo denotaremos por $\ominus P$. Y de hecho se tiene
$$\ominus P = (\mathcal{O} * \mathcal{O}) * P.$$

(iv) $\forall P, Q, R \in E(K)$ se tiene
$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

*Demostracion*:

(i) Por definición,
$$P \oplus \mathcal{O} := \mathcal{O} * (P * \mathcal{O}).$$
Utilizando la observación 1.6.1 tenemos que
$$\mathcal{O} * (P * \mathcal{O}) = (P * \mathcal{O}) * \mathcal{O} = \mathcal{O}.$$

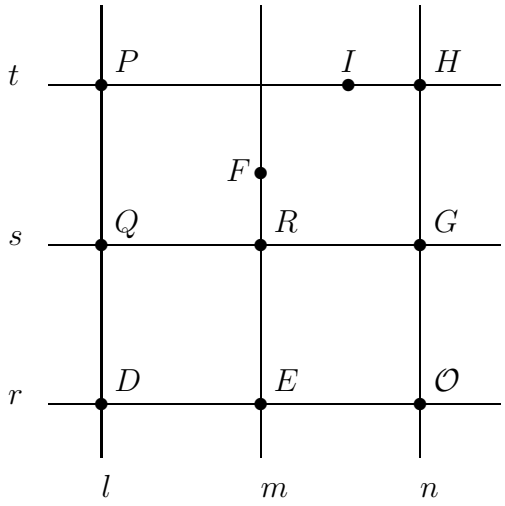
(ii) Es obvio por la construcción de $\oplus$ y por la observación 1.6.1 que

$$P \oplus Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q \oplus P.$$

(iii) Definimos $\ominus P := (\mathcal{O} * \mathcal{O}) * P$. Entonces utilizando de nuevo la observación 1.6.1 y la definición de $\oplus$,

$$P \oplus (\ominus P) = \mathcal{O} * [(\mathcal{O} * \mathcal{O}) * P) * P] = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O}.$$

(iv) Sean $P, Q, R \in E(K)$. Consideramos el diagrama siguiente




En el diagrama $r, s, t, l, m, n$ son rectas y el resto de las letras son puntos de $E(K)$. Dichos puntos son intersecciones de dos de las rectas excepto, en principio, $F$ e $I$. $(P \oplus Q) \oplus R$ es el tercer punto de intersección de la recta que une $F$ con $\mathcal{O}$, con $E$. Similarmente, $P \oplus (Q \oplus R)$ es el tercer punto de intersección de la recta que une $I$ con $\mathcal{O}$, con $E$.

Para probar la asociatividad, hemos de mostrar que $F$ e $I$ no son como muestra la anterior figura, sino que coinciden con el punto de intersección de las rectas $m$ y $t$. Se tiene por la definición de $\oplus$ que

$$\begin{array}{rcl} H & = & Q \oplus R, \\ E & = & P \oplus Q. \end{array}$$

Consideramos las cúbicas

$$\left\{ \begin{array}{rcl} G_1 & = & r \cdot s \cdot t, \\ G_2 & = & l \cdot m \cdot n. \end{array} \right.$$

Se observa que $P, Q, R, G, D, E, \mathcal{O}, H \in G_1 \cap G_2$. Además

$$\left\{ \begin{array}{l} F \in G_2, \\ I \in G_1. \end{array} \right.$$

Queremos demostrar que $I = F$, y lo haremos por reducción al absurdo. Supongamos que $I \neq F$. Si suponemos que $F \in G_1$ e $I \in G_2$ tenemos que $\#G_i \cap E(K) = 10$, $i = 1, 2$ en contradicción con el Teorema de Bézout que nos dice que es igual a 9. Por lo tanto,

$$F \notin G_1 \quad \text{ó} \quad I \notin G_2.$$

Para ver que $F = I$ utilizaremos el teorema 1.6.2. Tenemos que $G_1$ y $G_2$ pasan por 8 puntos de $E(K) \subset \mathbb{P}^2$. Estos 8 puntos están en posición general ya que:

- Si cuatro puntos están en una recta $L$, como además pertenecen a $E(K)$,

$$\sum_{P \in L \cap E(K)} I_P(E(K), L) \geq 4,$$

  en contradicción con el Teorema de Bézout.

- Si siete puntos pertenecen a una cónica, como también pertenecen a la curva elíptica $E(K)$, contradirían el Teorema de Bézout. Ya que si denotamos por $C$ a la cónica, obtenemos

$$\sum_{P \in C \cap E(K)} I_P(E(K), C) = 2 \cdot 3 = 6 < 7.$$

Por lo tanto estamos en las hipótesis de el Teorema 1.6.2. $G_1$ y $G_2$ pasan por los 8 puntos y un noveno distinto de $I$ y $F$, en contradicción con el Teorema de Bézout. Esto nos dice que $I = F$. Ya que por el teorema 1.6.2, dadas dos cúbicas en $\mathbb{P}^2$ que tienen 8 puntos en común entonces tienen un noveno en común. Por lo tanto hemos demostrado que

$$(P \oplus Q) * R = (Q \oplus R) * P. \tag{1.15}$$

Y obtenemos usando la identidad (1.15) junto con la propiedad $(ii)$ que

$$(P \oplus Q) \oplus R = \mathcal{O} * [(P \oplus Q) * R] = \mathcal{O} * [(Q \oplus R) * P] = (Q \oplus R) \oplus P = P \oplus (Q \oplus R).$$

□

Las propiedades de $\oplus$ nos van a dar el siguiente resultado:

**Proposición 1.6.3** *Sea $(E, \mathcal{O})$ una curva elíptica definida sobre $K$. Entonces $(E(K), \oplus)$ es un grupo abeliano con elemento neutro $\mathcal{O}$.*

*Demostración*: Es una consecuencia de las propiedades de $\oplus$, debido a que éstas nos indican que:

(i) $\mathcal{O}$ es el elemento neutro de $(E(K), \oplus)$.

(ii) $\oplus$ es conmutativa.

(iii) Todo elemento $P \in E(K)$ tiene un inverso con respecto a $\oplus$. Dicho elemento es $\ominus P$ y se tiene que

$$P \oplus (\ominus P) = \mathcal{O}.$$

(iv) $\oplus$ es asociativa.

□

**Observación 1.6.4** Si $\mathcal{O}' \in E(K)$ podemos formar el grupo abeliano $(E(K), \oplus')$. Definimos, de forma análoga a $\oplus$, la ley de grupo $\oplus'$:

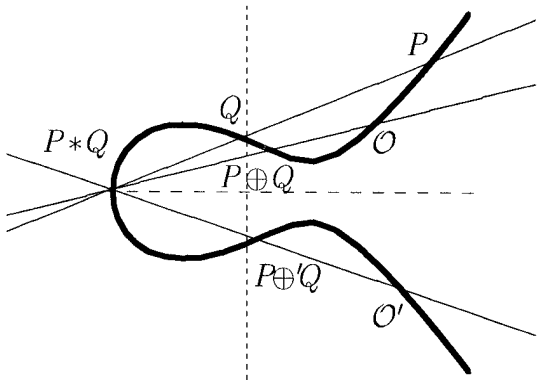
$$P \oplus' Q := \mathcal{O}' * (P * Q).$$

Pero,

¿ qué relación existe entre $(E(K), \oplus)$ y $(E(K), \oplus')$ ?

Queremos comparar

$$\begin{array}{rcl} P \oplus Q & = & \mathcal{O} * (P * Q) \\ & y & \\ P \oplus' Q & = & \mathcal{O}' * (P * Q). \end{array}$$




Tenemos

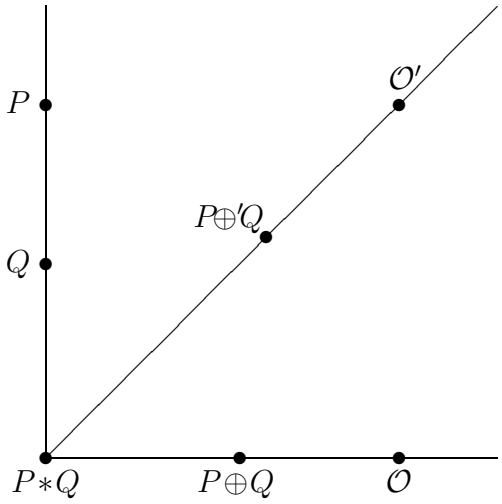
$$\boxed{(P \oplus' Q) \oplus \mathcal{O}' = P \oplus Q}$$

ya que

$$(P \oplus' Q) \oplus \mathcal{O}' = (\mathcal{O}' * (P * Q)) \oplus \mathcal{O}' = \mathcal{O} * [(\mathcal{O}' * (P * Q)) * \mathcal{O}'] = \mathcal{O} * (P * Q) = P \oplus Q.$$

Por lo tanto,

$$\boxed{P \oplus' Q = P \oplus Q \oplus (\ominus \mathcal{O}')}$$




La relación por la que nos preguntábamos antes está recogida en la siguiente proposición.

**Proposición 1.6.5** $(E(K), \oplus) \cong (E(K), \oplus')$.

*Demostración*: La siguiente aplicación:

$$\begin{array}{rccc} \varphi: & (E(K), \oplus) & \longrightarrow & (E(K), \oplus') \\ & P & \longmapsto & P \oplus \mathcal{O}' \end{array}$$

es isomorfismo de grupos. Primero vamos a ver que es un morfismo de grupos:

$$\begin{array}{rl} \varphi(P \oplus Q) & = (P \oplus Q) \oplus \mathcal{O}' = (P \oplus \mathcal{O}') \oplus (Q \oplus \mathcal{O}') \oplus (\ominus \mathcal{O}') = \\ & \varphi(P) \oplus \varphi(Q) \oplus (\ominus \mathcal{O}') = \varphi(P) \oplus' \varphi(Q), \end{array}$$

y

$$\varphi(\mathcal{O}) = \mathcal{O} \oplus \mathcal{O}' = \mathcal{O}'.$$

Ahora veamos que $\varphi$ es biyectiva:

- Inyectiva:
$$\varphi(P) = \mathcal{O}' \Longrightarrow P \oplus \mathcal{O}' = \mathcal{O}' \Longrightarrow P = \mathcal{O}.$$

- Sobreyectiva:

$$Q \in (E(K), \oplus') \Longrightarrow \varphi(Q \oplus (\ominus \mathcal{O}')) = Q \oplus (\ominus \mathcal{O}') \oplus \mathcal{O}' = Q.$$

Entonces si $P = Q \oplus (\ominus \mathcal{O}') \in (E(K), \oplus)$, se tiene

$$\varphi(P) = Q.$$

□

**Observación 1.6.6** Si $\mathcal{O}$ es un punto de inflexión[5] de $E(K)$, se tiene

$$\mathcal{O} * \mathcal{O} = \mathcal{O},$$

y por lo tanto,

$$\ominus P = P * \mathcal{O}.$$

Y además

$$P \oplus Q \oplus R = \mathcal{O} \Longleftrightarrow P, Q, R \text{ están alineados.}$$

Veámoslo:

$$P \oplus Q \oplus R = \mathcal{O} \Longleftrightarrow R = \ominus(P \oplus Q) = (P \oplus Q) * \mathcal{O} = (\mathcal{O} * (P * Q)) * \mathcal{O} = P * Q,$$

donde en la última igualdad hemos usado la observación 1.6.1.

□

### 1.6.1 Forma explícita de la ley de grupo.

Es conveniente tener la ley de grupo en forma explícita y en este apartado vamos a hallarla.

Una curva elíptica $E$ es una curva proyectiva lisa definida por un polinomio homogéneo de grado 3 junto con un punto $\mathcal{O} \in E$. Vimos que en estas condiciones podíamos encontrar, utilizando el algoritmo de Weierstrass, un isomorfismo de tal forma que

$$E(K) \cong \{[x, y, z] \in \mathbb{P}^2(K) : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\}.$$

También vimos que el único punto en el infinito de una ecuación de Weierstrass era $\mathcal{O} = [x, y, z]$. Por lo que podíamos poner

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}.$$

Vimos en la sección anterior que la ley de grupo era

$$P \oplus Q = \mathcal{O} * (P * Q).$$

Al tener $E(K)$ en forma de Weierstrass, vamos a poder escribir de forma sencilla y explícita la ley de grupo en $E(K)$.

**Nota** : Vamos a considerar[6] $car(\overline{K}) \neq 2$.

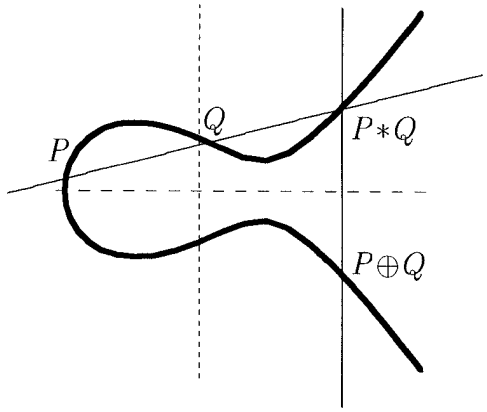
Considerando la nota anterior, $E(K)$ va a ser de la forma:

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax^2 + bx + c\} \cup \{[0, 1, 0]\}.$$

[5]Es el caso que más nos va a interesar, ya que cuando tengamos a $E$ en su ecuación de Weierstrass, el punto $[0, 1, 0]$ que denotábamos por $\mathcal{O}$ será un punto de inflexión.

[6]Para el caso especial en el que $car(\overline{K}) = 2$ ver [SIL], Apéndice A.

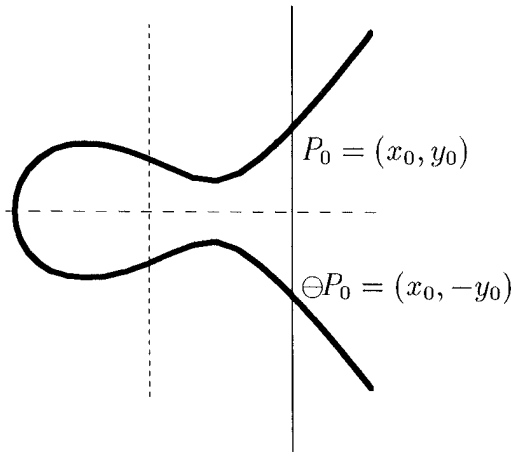
La ley de grupo cuando $E(K)$ está dada de esta forma va a ser gráficamente




Vimos en la observación 1.5.3 que el punto $\mathcal{O} = [0, 1, 0]$ siempre era un punto de inflexión de $E(K)$ cuando $E(K)$ venía dada por una ecuación de Weierstrass. Así si $P = (x_0, y_0) \in E(K)$ se tiene que

$$\ominus P = (x_0, -y_0).$$

Gráficamente,




Ahora, si $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ con $P_1 \neq P_2$ denotaremos

$$P_1 * P_2 = (x_3, y_3).$$

Vamos a hallar $(x_3, y_3)$. Primero hallamos la recta que une $(x_1, y_1)$ con $(x_2, y_2)$.

Esta recta tiene como ecuación

$$y = \lambda x + \nu, \quad \text{con} \quad \begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}, \\ \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2. \end{cases}$$

Por construcción, la recta interseca a la cúbica en tres puntos, $(x_1, y_1), (x_2, y_2)$ y $(x_3, y_3)$. Sustituyendo tenemos

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c,$$

es decir,

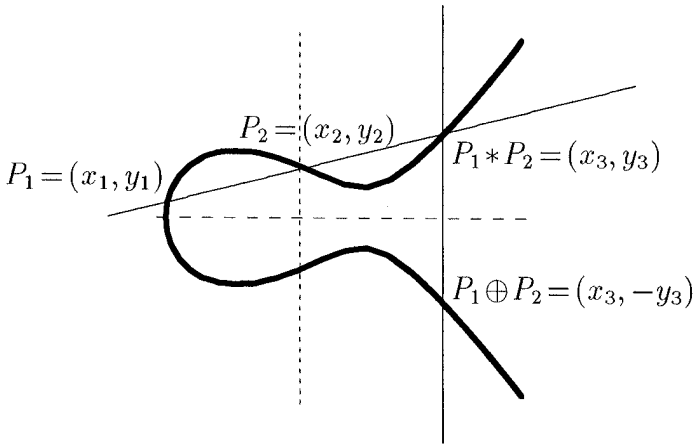
$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0.$$

Ésta es una ecuación cúbica en $x$, y sus tres raíces son $x_1, x_2, x_3$:

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3)$$

por lo que podemos hallar $x_3$ igualando los coeficientes. Si igualamos los coeficientes de $x^2$ en ambos lados, obtenemos

$$\boxed{\begin{cases} x_3 = \lambda^2 - a - x_1 - x_2 \\ y_3 = \lambda x_3 + \nu \end{cases}}$$




Analizaremos ahora el caso $P_1 = P_2$. Llamemos $P_0 = (x_0, y_0)$ y calculemos $[2]P_0 = P_0 \oplus P_0$. Como $x_1 = x_2$ e $y_1 = y_2$ no podemos usar la fórmula anterior para $\lambda$, por lo que debemos tomar la recta tangente a $E(K)$ que pasa por $P_0$. De la relación $y^2 = f(x) = x^3 + ax^2 + bx + c$, derivando implícitamente, obtenemos

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}.$$

Denotando $[2]P_0 = (x([2]P_0), y([2]P_0))$ y $\nu = y_0 - \lambda x_0$, obtenemos

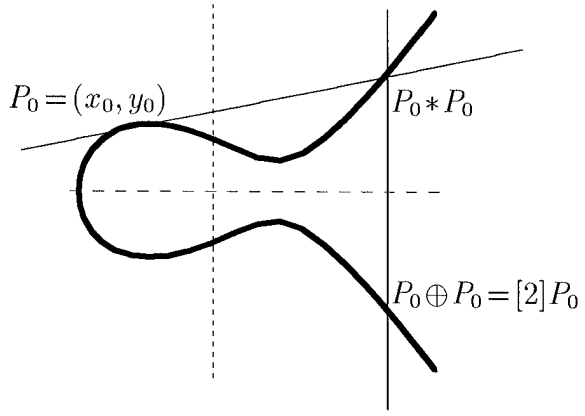
$$\boxed{\begin{cases} x([2]P_0) &= \lambda^2 - a - 2x_0, \\ y([2]P_0) &= \lambda x([2]P_0) + \nu. \end{cases}}$$

Si escribimos de forma explícita el valor de $\lambda$, esto es,

$$\lambda = \frac{3x^2 + 2ax + b}{2y},$$

conseguimos una fórmula explícita de $[2]P_0 = (x([2]P_0), y([2]P_0))$:

$$\boxed{\begin{cases} x([2]P_0) = \dfrac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c} \\ \\ y([2]P_0) = \left(\dfrac{3x_0^2 + 2ax_0 + b}{2y_0}\right) x([2]P_0) + y_0 - \left(\dfrac{3x_0^2 + 2ax_0 + b}{2y_0}\right) x_0 \end{cases}}$$




Por lo tanto, si nuestra curva elíptica $E$ está dada por $y^2 = f(x) = x^3 + ax^2 + bx + c$ y si $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_1 \oplus P_2 = (x_3, y_3)$ entonces

$$\boxed{\begin{cases} x_3 &= \lambda^2 - a - x_1 - x_2 \\ y_3 &= \lambda x_3 + \nu \end{cases} \quad \text{con} \quad \begin{cases} \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & si \quad P_1 \neq P_2 \\ \\ \dfrac{f'(x_1)}{2y_1} & si \quad P_1 = P_2 \end{cases} \\ \\ \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2 \end{cases}} \tag{1.16}$$

### 1.6.2 Ley de grupo en una cúbica irreducible singular.

Para completar nuestro estudio general de las cúbicas irreducibles, en este apartado estudiaremos las cúbicas irreducibles singulares. Introduciremos una ley de grupo en la parte no singular de una cúbica irreducible singular dada por una ecuación de Weierstrass.

**Definición.** *Sea $C$ una curva cúbica (puede ser singular) dada por una ecuación de Weierstrass. La* **parte no singular de** *$C$, que denotaremos por $C_{ns}$, es el conjunto de puntos no singulares de $C$.*

*Similarmente, si $C$ está definida sobre $K$, entonces $C_{ns}(K)$ es el conjunto de puntos no singulares de $C(K)$.*

Vamos a dotar a $C_{ns}(K)$ de estructura de grupo. Vimos que $\mathcal{O} \in C_{ns}(K) \subseteq C(K)$. Si $P, Q \in C_{ns}(K)$ nos preguntamos:

$$¿P * Q \in C_{ns}(K)\ ?$$

La respuesta es que sí: supongamos que $P * Q$ es singular, y sea $L$ la recta que une $P, Q$ y $P * Q$. Por el Teorema de Bézout,

$$\sum_{P' \in L \cap C(K)} I_{P'}(L, C(K)) \geq 4,$$

con lo que llegamos a una contradicción. Pero si $C$ es singular vamos a poder decir aún más.

**Proposición 1.6.7** *Sea $C$ una curva cúbica dada por una ecuación de Weierstrass con discriminante $\Delta = 0$. Es decir, $C$ es singular y por lo tanto $C$ tiene un único punto singular $S$. Entonces la ley de composición $\oplus$,*

$$P \oplus Q := \mathcal{O} * (P * Q) \quad P, Q \in C_{ns}(K),$$

*convierte a $(C_{ns}(K), \oplus)$ en un grupo abeliano. Además podemos decir cómo va a ser la estructura de grupo en $K$.*

*(i) Supongamos que $S$ es un nodo, y sean*

$$y = \alpha_1 x + \beta_1 \quad e \quad y = \alpha_2 x + \beta_2$$

*las dos rectas tangentes a $C(K)$ en $S$. Entonces la aplicación*

$$\begin{array}{rcl} C_{ns}(\overline{K}) & \longrightarrow & (\overline{K}^*, \bullet) \\ (x, y) & \longmapsto & \frac{y - \alpha_1 x + \beta_1}{y - \alpha_2 x + \beta_2} \end{array}$$

*es un isomorfismo de grupos abelianos.*

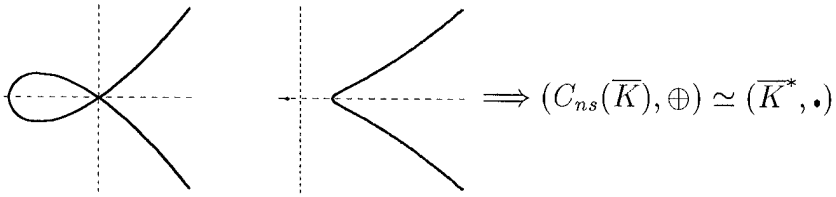
*(ii) Supongamos que $S$ es una cúspide, y sea $y = \alpha x + \beta$ la*[7] *recta tangente a $E(K)$ en $S$. Entonces la aplicación*

$$\begin{array}{rcl} C_{ns}(\overline{K}) & \longrightarrow & (\overline{K}^{+}, +) \\ (x, y) & \longmapsto & \frac{x - x(S)}{y - \alpha x - \beta} \end{array}$$

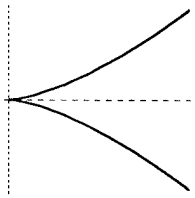
*es un isomorfismo de grupos abelianos.*

*Demostración*: Ver [SIL], Capítulo III, Proposición 2.5.

**Observación 1.6.8** La proposición anterior nos dice:



$\Longrightarrow (C_{ns}(\overline{K}), \oplus) \simeq (\overline{K}^{*}, \cdot)$



$\Longrightarrow (C_{ns}(\overline{K}), \oplus) \simeq (\overline{K}^{+}, +)$

[7] Si $S$ es un nodo las dos rectas son distintas, mientras que si $S$ es una cúspide sólo hay una recta tangente.

# Capítulo 2

# Geometría algebraica y curvas elípticas.

En este capítulo desarrollaremos una serie de conceptos generales de Geometría Algebraica. Con ellos daremos una definición más general de curva elíptica. Veremos que la teoría desarrollada en el capítulo anterior no es más que una aplicación de la teoría expuesta aquí. Además veremos que la definición de curva elíptica como una curva cúbica proyectiva lisa junto con un punto perteneciente a ella, es equivalente a la que daremos en este capítulo.

La mayor parte de este capítulo será una mera reseña de definiciones y resultados, en su mayor parte sin demostración, que necesitaremos para probar la equivalencia entre la definición de curva elíptica dada aquí y la que dimos en el capítulo anterior.

## 2.1 Variedades algebraicas.

Sea $\overline{K}[x] = \overline{K}[x_1, \ldots, x_n]$ el anillo de los polinomios en $n$ variables, con $K$ un cuerpo perfecto y $\overline{K}$ un cierre algebraico fijo de $K$. Sea $I \subset \overline{K}[x]$ un ideal. A cada ideal $I$ le asociamos el conjunto

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \quad \forall f \in I\},$$

con $\mathbb{A}^n = \{P = (x_1, \ldots, x_n) : x_i \in \overline{K} \quad \forall i\}$.

**Definición.** *Un* **conjunto algebraico (afín)** *es cualquier conjunto de la forma $V_I$. Si $V$ es un conjunto algebraico afín, el* **ideal de V** *está dado por*

$$I(V) = \{f \in \overline{K}[x] : f(P) = 0 \quad \forall P \in V\}.$$

**Observación 2.1.1** Sea $J \subset \overline{K}[x]$ un ideal, entonces

$$I(V_J) = radical(J) = \{f \in \overline{K}[x] : \exists n \in \mathbb{N} \text{ tal que } f^n \in J\}.$$

**Observación 2.1.2** El teorema de las bases de Hilbert nos dice que todo ideal de $K[x]$ y de $\overline{K}[x]$ está finitamente generado. En particular, $I(V)$ está finitamente generado.

Un conjunto algebraico afín se dice **definido sobre** $K$ si su ideal $I(V)$ puede ser generado por polinomios en $K[x]$; lo denotaremos por $V/K$. Si definimos

$$I(V/K) = \{f \in K[x] : f(P) = 0 \ \forall P \in V\} = I(V) \cap K[x],$$

entonces

$$V \text{ definido sobre } K \iff I(V) = I(V/K)\overline{K}[x].$$

Si $V$ está definido sobre $K$, el conjunto de **puntos racionales de** $V$ **sobre** $K$ es

$$V(K) = V \cap \mathbb{A}^n(K),$$

donde $\mathbb{A}^n(K) = \{P \in \mathbb{A}^n : x_i \in K \quad \forall i\}$. En este caso, si $f_1, \ldots, f_n \in K[x]$ son generadores de $I(V/K)$, entonces

$$V(K) = \{x = (x_1, \ldots, x_n) \in \mathbb{A}^n(K) : f_1(x) = \ldots = f_n(x) = 0\}.$$

**Observación 2.1.3** El grupo de Galois de $\overline{K}$ sobre $K$, denotado por $Gal(\overline{K}/K)$, actúa en $\mathbb{A}^n$; sea $\sigma \in Gal(\overline{K}/K)$ y $P = (x_1, \ldots, x_n) \in \mathbb{A}^n$, entonces

$$P^\sigma = (x_1^\sigma, \ldots, x_n^\sigma) = (\sigma(x_1), \ldots, \sigma(x_n)).$$

Entonces $\mathbb{A}^n(K)$ puede ser caracterizado por

$$\mathbb{A}^n(K) = \{P \in \mathbb{A}^n : P^\sigma = P \quad \forall \sigma \in Gal(\overline{K}/K)\}.$$

Además, si tenemos $f(x) \in K[x]$ y $P \in \mathbb{A}^n$, entonces para cualquier $\sigma \in Gal(\overline{K}/K)$,

$$f(P^\sigma) = f(P)^\sigma.$$

Entonces, si $V$ es un conjunto algebraico definido sobre $K$, la acción de $Gal(\overline{K}/K)$ en $\mathbb{A}^n$ induce una acción en $V$, y se obtiene

$$V(K) = \{P \in V : P^\sigma = P \quad \forall \sigma \in Gal(\overline{K}/K)\}.$$

**Definición.** *Un conjunto algebraico afín $V$ se dice que es una* **variedad algebraica (afín)** *si $I(V)$ es un ideal primo en $\overline{K}[x]$.*

**Definición.** *Se define el* **anillo de coordenadas afines de** $V/K$ *como*

$$K[V] := K[x]/I(V/K).$$

*Éste es un dominio, su cuerpo de cocientes se denota por $K(V)$ y se denomina* **cuerpo de funciones de** $V$*. Definiciones análogas se tienen para $\overline{K}[V]$ y $\overline{K}(V)$, reemplazando $K$ por $\overline{K}$.*

**Definición.** *Sea $V$ una variedad algebraica. La* **dimensión de** $V$*, denotada por $dim(V)$, es el grado de trascendencia de $\overline{K}(V)$ sobre $\overline{K}$.*

**Observación 2.1.4** Si $V \subset \mathbb{A}^n$ está dada por una sóla ecuación polinómica no constante $f(x_1, \ldots, x_n) = 0$, entonces

$$dim(V) = n - 1.$$

El recíproco también es cierto.

**Definición.** *Sea $V$ una variedad algebraica, $P \in V$ y $f_1, \ldots, f_m \in \overline{K}[x]$ un conjunto de generadores de $I(V)$. Decimos que $V$ es* **no singular (o lisa) en** *$P$ si la matriz $m \times n$*

$$\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{\substack{i=1.\ \ldots,m \\ j=1,\ \ldots,n}} \quad \text{tiene rango } n - dim(V).$$

*Si $V$ es no singular en todo punto, diremos que $V$ es* **lisa**.

**Ejemplo 2.1.1** Sea $V = \{x \in \mathbb{A}^n(K) : f(x) = 0\}$; entonces $dim(V) = n - 1$ y además

$$P \in V \text{ es singular} \iff \frac{\partial f}{\partial x_i}(P) = 0 \quad \forall i = 1, \ldots, n.$$

Podemos hacer otra caracterización de suavidad en términos de las funciones en la variedad $V$. Sea $P \in V$, y definamos el ideal $M_P$ en $\overline{K}[V]$ mediante

$$M_P := \{f \in \overline{K}[V] : f(P) = 0\}.$$

Se obtiene que $M_P$ es un ideal maximal y que $M_P/{M_P}^2$ es un $\overline{K}$-espacio vectorial de dimensión finita.

**Proposición 2.1.5** *Sea $V$ una variedad algebraica. Entonces*

$$P \in V \text{ es no singular} \iff dim_{\overline{K}}\left(M_P/{M_P}^2\right) = dim(V).$$

*Demostración*: Ver [HAR], Capítulo I, Teorema 5.1.

**Definición.** *Sea $V$ una variedad algebraica y $P \in V$. Llamaremos el* **anillo local de $V$ en** *$P$, denotado por $\overline{K}[V]_P$ ó $\mathcal{O}_{V,P}$, a la localización de $\overline{K}[V]$ en $M_P$. Es decir,*

$$\overline{K}[V]_P := \{F \in \overline{K}(V) : F = f/g \text{ con } f, g \in \overline{K}[V] \text{ y } g(P) \neq 0\}.$$

*Si $F = f/g \in \overline{K}[V]_P$, entonces $F(P) = f(P)/g(P)$ está bien definida. Las funciones de $\overline{K}[V]_P$ se llaman* **regulares (o definidas) en** *$P$.*

## 2.2 Variedades proyectivas.

**Definición.** *Un polinomio* $f \in \overline{K}[x] = \overline{K}[x_0 \ldots, x_n]$ *es* **homogéneo de grado** $d$ *si*

$$f(\lambda x_0, \ldots, \lambda x_0) = \lambda^d f(x_0, \ldots, x_n) \quad \forall \lambda \in \overline{K}.$$

*Un ideal* $I \subset \overline{K}[x]$ *es* **homogéneo** *si está generado por polinomios homogéneos.*

A cada ideal homogéneo $I$, le asociamos el subconjunto de $\mathbb{P}^n$

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 \quad \forall f \in I \text{ homogéneo}\}.$$

**Definición.** *Un* **conjunto algebraico proyectivo** *es cualquier conjunto de la forma* $V_I$.

*Si* $V$ *es un conjunto algebraico proyectivo, el* **ideal homogéneo de** $V$ *es el ideal, denotado por* $I(V)$*, generado por*

$$\{f \in \overline{K}[x] : f \text{ es homogéneo y } f(P) = 0 \quad \forall P \in V\}.$$

$V$ *es* **definido sobre** $K$*, y lo denotaremos por* $V/K$*, si su ideal* $I(V)$ *está generado por polinomios homogéneos en* $K[x]$*. Si tenemos* $V/K$*, el conjunto de los* **puntos racionales de** $V$ *es*

$$V(K) = V \cap \mathbb{P}^n(K).$$

**Ejemplo 2.2.1** Una *recta* en $\mathbb{P}^2$ es

$$L := \{[x, y, z] \in \mathbb{P}^2 : ax + by + cz = 0, \quad a, b, c \in \overline{K} \text{ no todos } 0\}.$$

En general, el equivalente en $\mathbb{P}^n$ a una recta en $\mathbb{P}^2$, un *hiperplano* en $\mathbb{P}^n$ es

$$H = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : a_0x_0 + \ldots + a_nx_n = 0, \quad a_0, \ldots, a_n \in \overline{K} \text{ no todos } 0\}.$$

**Definición.** *Un conjunto algebraico proyectivo* $V$ *se dice que es una* **variedad proyectiva** *si su ideal homogéneo* $I(V)$ *es un ideal primo en* $\overline{K}[x]$.

**Observación 2.2.1** El grupo de Galois actua en $\mathbb{P}^n$ mediante la acción sobre las coordenadas homogéneas; sea $P = [x_0, \ldots, x_n] \in \mathbb{P}^n$ y $\sigma \in Gal(\overline{K}/K)$, entonces

$$[x_0, \ldots, x_n]^\sigma = [x_0^\sigma, \ldots, x_n^\sigma].$$

Sean

$$\begin{array}{rccc} \phi_i & : & \mathbb{A}^n & \hookrightarrow & \mathbb{P}^n \\ & & (y_1, \ldots, y_n) & \mapsto & [y_1, \ldots, y_{i-1}, 1, y_i, \ldots, y_n]. \end{array}$$

Con estas aplicaciones vemos que $\mathbb{P}^n$ tiene varias copias de $\mathbb{A}^n$.

Sea $H_i$ el hiperplano de $\mathbb{P}^n$ dado por $x_i = 0$, y consideramos

$$U_i = \mathbb{P}^n \setminus H_i = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : x_i \neq 0\}.$$

Se tiene entonces una biyección natural

$$\begin{array}{rccccc} {\phi_i}^{-1} & : & U_i & \longrightarrow & \mathbb{A}^n & i = 0, \ldots, n. \\ & & [x_1, \ldots, x_n] & \longmapsto & \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right) & \end{array}$$

Sea $V$ un conjunto algebraico proyectivo con ideal homogéneo $I(V)$, entonces $V \cap \mathbb{A}^n$ (e.d. $\phi_i^{-1}(V \cap U_i)$) es un conjunto algebraico afín con ideal

$$I(V \cap \mathbb{A}^n) \subset \overline{K}[y] = \overline{K}[y_1, \ldots, y_n]$$

dado por

$$I(V \cap \mathbb{A}^n) = \{f(y_1, \ldots, y_{i-1}, 1, y_i, \ldots, y_n) : f(x_0, \ldots, x_n) \in I(V)\}.$$

Observamos que por la definición del conjunto $U_i$ se tiene que

$$\bigcup_{i=0}^{n} U_i = \mathbb{P}^n.$$

Entonces toda variedad proyectiva $V$ tiene un cubrimiento por subconjuntos de la forma $V \cap U_0, \ldots, V \cap U_n$. Cada uno de ellos es una variedad afín vía la aplicación ${\phi_i}^{-1}$ correspondiente.

El proceso de reemplazar $f(x_0, \ldots, x_n)$ por $f(y_1, \ldots, y_{i-1}, 1, y_i, \ldots, y_n)$ se denomina **deshomogenización con respecto a** $x_i$. El proceso inverso es el siguiente: dado $f(y) \in \overline{K}[y]$ de grado $d$, definimos

$$f^*(x_0, \ldots, x_n) = {x_i}^d f\left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

Decimos que $f^*$ **es una homogenización de** $f$ **con respecto a** $x_i$.

En lo que sigue, fijamos $i$.

**Definición.** *Sea $V$ un conjunto algebraico afín con ideal $I(V)$. Consideramos $V$ como un subconjunto de $\mathbb{P}^n$ mediante la aplicación $\phi : V \subset \mathbb{A}^n \longrightarrow \mathbb{P}^n$. La* **clausura proyectiva de** *$V$, denotada por $\overline{V}$, es el conjunto algebraico proyectivo cuyo ideal homogéneo $I(\overline{V})$ está generado por el conjunto*

$$\{f^*(x) : f \in I(V)\}.$$

**Proposición 2.2.2**

*(i) Sea $V$ una variedad afín. Entonces $\overline{V}$ es una variedad proyectiva y además*

$$V = \overline{V} \cap \mathbb{A}^n.$$

*(ii) Sea $V$ una variedad proyectiva. Entonces $V \cap \mathbb{A}^n$ es una variedad afín y se tiene*

$$V \cap \mathbb{A}^n = \emptyset \quad ó \quad \overline{V \cap \mathbb{A}^n} = V.$$

*(iii) Si una variedad afín (respectivamente proyectiva) $V$ está definida sobre $K$, entonces $\overline{V}$ (respectivamente $V \cap \mathbb{A}^n$) está definida sobre $K$.*

*Demostración*: Ver [HAR], Capítulo I, Corolario 2.3.

**Observación 2.2.3** La proposición anterior nos dice que cada variedad afín está identificada con una única variedad proyectiva.

Sea $V$ una variedad afín y $\overline{V}$ su clausura; entonces diremos que $\overline{V} \setminus V$ son los **puntos en el infinito de** $V$.

**Definición.** *Sea $V/K$ una variedad proyectiva, y elijamos un representante de $\mathbb{A}^n$ dentro de $\mathbb{P}^n$ tal que $V \cap \mathbb{A}^n \neq \emptyset$. Definimos la* **dimensión de** *$V$, denotada por $dim(V)$, como*

$$dim(V) = dim(V \cap \mathbb{A}^n).$$

*El* **cuerpo de funciones de** *$V$, denotado por $K(V)$, es el cuerpo de funciones de $V \cap \mathbb{A}^n$ (de forma análoga para $\overline{K}(V)$). Sea $P \in V$ tal que $P \in \mathbb{A}^n$. Se dice que $V$ es* **no singular (o lisa) en** *$P$ si $V \cap \mathbb{A}^n$ es no singular en $P$. El* **anillo local de** *$V$* **en** *$P$, denotado por $K[V]_P$, es el anillo local de $V \cap \mathbb{A}^n$. Una función $F \in K(V)$ es* **regular (o definida) en** *$P$ si $F \in K[V]_P$.*

**Observación 2.2.4** El cuerpo de funciones de $\mathbb{P}^n$ puede ser descrito como el subcuerpo de $\overline{K}(x_0, \ldots, x_n)$ de funciones racionales $F(x) = f(x)/g(x)$ con $f$ y $g$ polinomios homogéneos del mismo grado.

Igualmente, el cuerpo de funciones de una variedad proyectiva $V$ es el cuerpo de funciones racionales $F(x) = f(x)/g(x)$ tales que:

(i) $f$ y $g$ son polinomios homogéneos del mismo grado.

(ii) $g \notin I(V)$.

(iii) Dos funciones $f/g$ y $f'/g'$ están identificadas si $fg' - f'g \in I(V)$.

## 2.3 Aplicaciones entre variedades proyectivas.

En este apartado generalizaremos la noción de aplicación racional entre curvas, dada en la sección §1.5, a variedades proyectivas arbitrarias. Y veremos algunos resultados sobre éstas.

**Definición.** *Sean $V_1 \subset \mathbb{P}^m$ y $V_2 \subset \mathbb{P}^n$ variedades proyectivas. Una* **aplicación racional entre $V_1$ y $V_2$** *es una aplicación de la forma*

$$\begin{aligned} \phi : V_1 &\longrightarrow V_2 \\ \phi &= [f_0, \ldots, f_n], \end{aligned}$$

*donde $f_0, \ldots, f_n \in \overline{K}(V_1)$ tienen la propiedad de que para todo $P \in V_1$ donde $f_0, \ldots, f_n$ estén definidas*

$$\phi(P) = [f_0(P), \ldots, f_n(P)] \in V_2.$$

*Además si $\exists \lambda \in \overline{K}^*$ tal que $\lambda f_0, \ldots, \lambda f_n \in K(V_1)$, entonces se dice que $\phi$ está* **definida sobre $K$.**

**Observación 2.3.1** Una aplicación racional $\phi : V_1 \longrightarrow V_2$ no está necesariamente definida en todos los puntos de $V_1$. Sin embargo, a veces es posible evaluar $\phi$ en puntos $P$ de $V_1$ donde algún $f_i$ no es regular, reemplazando $f_i$ por $gf_i$, con una función apropiada $g \in \overline{K}(V_1)$.

**Definición.** *Una aplicación $\phi = [f_0, \ldots, f_n] : V_1 \longrightarrow V_2$ se dice que es* **regular (o definida) en $P \in V_1$,** *si $\exists\, g \in \overline{K}(V_1)$ tal que:*

*(i) Cada $gf_i$ es regular en $P$.*

*(ii) Para algún $i$, $(gf_i)(P) \neq 0$.*

*Si dicha $g$ existe, tendremos $\phi(P) = [(gf_0)(P), \ldots, (gf_n)(P)]$. A veces serán necesarias diferentes aplicaciones $g$ para diferentes puntos. Una aplicación racional que es regular en todo punto se dice que es un* **morfismo**.

Sean $V_1 \subset \mathbb{P}^m$ y $V_2 \subset \mathbb{P}^n$ variedades proyectivas. Sabemos por la observación 2.2.4 que las funciones en $\overline{K}(V_1)$ pueden ser descritas como cocientes de polinomios homogéneos de $\overline{K}[x_0, \ldots, x_m]$ del mismo grado. Entonces, si tenemos una aplicación racional $\phi = [f_0, \ldots, f_n]$, multiplicando las componentes de $\phi$ por el mínimo común múltiplo de los denominadores de $f_0, \ldots, f_n$, quitamos denominadores y así obtenemos la siguiente definición alternativa de aplicación racional
Una **aplicación racional** $\phi : V_1 \longrightarrow V_2$ es una aplicación de la forma $\phi = [\phi_0(x), \ldots, \phi_n(x)]$ tal que:

(i) $\phi_i(x) \in \overline{K}[x] = \overline{K}[x_0, \ldots, x_m]$ son polinomios homogéneos, no todos en $I(V_1)$, con el mismo grado.

(ii) Para todo $f \in I(V_2)$, $f(\phi_0(x), \ldots, \phi_n(x)) \in I(V_1)$.

Así $\phi(P)$ está bien definido siempre que $\phi_i(P) \neq 0$ para algún $i$. Además si $\phi_i(P) = 0\ \forall i$ es posible, a veces, "alterar"$\phi$ para que tenga sentido $\phi(P)$. Más precisamente, una aplicación racional $\phi = [\phi_0, \ldots, \phi_n] : V_1 \longrightarrow V_2$, como antes, es **regular (o definida) en** $P \in V_1$ si existen polinomios homogéneos $\psi_0, \ldots, \psi_n \in \overline{K}[x]$ tales que

(i) $\psi_0, \ldots, \psi_n$ tienen el mismo grado.

(ii) $\phi_i\psi_j = \phi_j\psi_i (mod\ I(V_1))$ para $0 \leq i, j \leq n$.

(iii) $\psi_i(P) \neq 0$ para algún $i$.

Entonces, $\phi(P) = [\psi_0(P), \ldots, \psi_n(P)]$.

**Observación 2.3.2** Sea $\phi = [\phi_0, \ldots, \phi_n] : \mathbb{P}^m \longrightarrow \mathbb{P}^n$ una aplicación racional, donde $\phi_i \in \overline{K}[x]$ son polinomios homogéneos del mismo grado. Como $\overline{K}[x]$ es un *D.F.U.*, podemos asumir que los $\phi_i$ no tienen factores comunes. Entonces obtenemos los siguientes resultados:

(i) $\phi$ es regular en $P \Longleftrightarrow$ algún $\phi_i \neq 0$.
Ya que como $I(\mathbb{P}^m) = (0)$ no hay forma de alterar los $\phi_i$.

(ii) $\phi$ es un morfismo $\Longleftrightarrow$ los $\phi_i$ no tienen ceros comunes en $\mathbb{P}^m$.
Por lo anterior.

**Definición.** *Sean $\phi, \varphi : V_1 \longrightarrow V_2$ dos aplicaciones racionales. Diremos que son* **equivalentes**, *$\phi \sim \varphi$, si para todo abierto $U \subseteq V_1$ distinto del vacío en el que $\phi$ y $\varphi$ estén definidas se tiene que $\phi|_U = \varphi|_U$.*

**Definición.** *Sean $V_1$ y $V_2$ variedades proyectivas. Diremos que $V_1$ y $V_2$ son* **birracionalmente equivalentes** *si existen aplicaciones racionales $\phi : V_1 \longrightarrow V_2$ y $\psi : V_2 \longrightarrow V_1$ tales que $\psi \circ \phi \sim 1_{V_1}$ y $\phi \circ \psi \sim 1_{V_2}$.*

*Además diremos que $V_1$ y $V_2$ son* **birracionalmente equivalentes sobre** *$K$ si $\phi$ y $\psi$ están definidas sobre $K$.*

*Diremos que $V_1$ y $V_2$ son* **isomorfas**, *$V_1 \cong V_2$, si $V_1$ y $V_2$ son birracionalmente equivalentes y las aplicaciones $\phi$ y $\psi$ son morfismos. Y diremos que son* **isomorfas sobre** *$K$, $V_1/K \cong V_2/K$, si $\phi$ y $\psi$ están definidas sobre $K$.*

**Observación 2.3.3** Si $\phi : V_1 \longrightarrow V_2$ es un isomorfismo definido sobre $K$, entonces $\phi$ identifica $V_1(K)$ y $V_2(K)$. En particular para estudiar problemas diofánticos es suficiente estudiar cualquier variedad en una clase de $\mathbb{Q}$-isomorfismos de variedades.

## 2.4 Aplicaciones entre curvas.

En esta sección, curva querrá decir variedad proyectiva de dimensión 1.

**Proposición 2.4.1** *Sea $C$ una curva y $P \in C$ un punto no singular. Entonces $\overline{K}[C]_P$ es un anillo de valoración discreta, con valoración:*

$$ord_P : \overline{K}[C]_P \longrightarrow \{0, 1, 2, \ldots\} \cup \{\infty\}$$
$$ord_P(f) = max\{d \in \mathbb{Z} : f \in M_P^d\}.$$

*Además definiendo*

$$ord_P(f/g) = ord_P(f) - ord_P(g),$$

*podemos extender $ord_P$ a $\overline{K}(C)$,*

$$ord_P : \overline{K}(C)_P \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

*Demostración*: Ver [A-M], Proposición 9.2.

**Definición.** *Un* **parámetro uniformizante para** *$P \in C$ es una función $t \in \overline{K}(C)$ con $ord_P(t) = 1$. Es decir, $t$ es un generador de $M_P$.*

**Proposición 2.4.2** *Sea $C/K$ una curva y $t \in K(C)$ un parámetro uniformizante en algún punto no singular $P \in C$. Entonces $K(C)$ es una extensión finita y separable de $K(t)$.*

*Demostración*: Ver [SIL], Capítulo II, Proposición 1.4.

**Proposición 2.4.3** *Sea $C$ una curva, $V \subset \mathbb{P}^N$ una variedad proyectiva, $P \in C$ un punto no singular, y $\phi : C \longrightarrow V$ una aplicación racional. Entonces $\phi$ es regular en $P$. En particular, si $C$ es lisa, entonces $\phi$ es un morfismo.*

*Demostración*: Sea $\phi = [f_0, \ldots, f_N]$ con $f_i \in \overline{K}(C)$, y $t \in \overline{K}(C)$ un parámetro uniformizante para $C$ en $P$. Y sea

$$n = \min_{0 \le i \le N} \{ord_P(f_i)\}.$$

Entonces

$$ord_P(t^{-n} f_i) \geq 0 \quad \forall i \in \{1, \ldots, N\} \qquad y \qquad ord_P(t^{-n} f_j) = 0 \text{ para algún } j.$$

Por lo tanto $t^{-n} f_i$ es regular en $P$ y $t^{-n} f_j(P) \neq 0$, esto es, $\phi$ es regular en $P$.

□

**Teorema 2.4.4** *Sea $\phi : C_1 \longrightarrow C_2$ un morfismo de curvas.*

$$\text{Entonces } \phi \text{ es} \begin{cases} \text{constante} \\ o \\ \text{sobreyectiva.} \end{cases}$$

*Demostración*: Ver [HAR], Capítulo II, Proposición 6.8.

Si tenemos dos curvas $C_1/K$ y $C_2/K$ y una aplicación racional $\phi : C_1 \longrightarrow C_2$ no constante definida sobre $K$, $\phi$ induce una aplicación entre los cuerpos de funciones de $C_1/K$ y $C_2/K$. Efectivamente, tenemos definido

$$\begin{array}{rcl} \phi^* : K(C_2) & \longrightarrow & K(C_1) \\ f & \longmapsto & \phi^*(f) := f \circ \phi. \end{array}$$

**Teorema 2.4.5** *Sean $C_1/K$ y $C_2/K$ dos curvas y sea $\phi : C_1 \longrightarrow C_2$ una aplicación racional no constante definida sobre $K$. Entonces $K(C_1)$ es una extensión finita de $\phi^* K(C_2)$.*

*Demostración*: Ver [HAR], Capítulo II, Proposición 6.8.

**Definición.** *Sea $\phi : C_1 \longrightarrow C_2$ una aplicación de curvas definida sobre $K$. Vamos a definir el* **grado de** *$\phi$ como:*

$$deg(\phi) = \begin{cases} 0 & si\ \phi\ es\ constante \\ [K(C_1) : \phi^* K(C_2)] & si\ \phi\ no\ es\ constante \end{cases}$$

*Se dice que $\phi$ es* **separable (inseparable , puramente inseparable)** *si la extensión $K(C_1)/\phi^* K(C_2)$ tiene la correspondiente propiedad.*

Por el teorema 2.4.5 se tiene que $deg(\phi) < \infty$, y contadas adecuadamente (ver proposición 2.4.7), el grado de $\phi$ nos dice cuántas imágenes inversas por $\phi$ tiene un punto de $C_2$.

**Proposición 2.4.6** *Sean $C_1$ y $C_2$ curvas lisas y sea $\phi : C_1 \longrightarrow C_2$ una aplicación racional.*

$$Si\ deg(\phi) = 1 \Longrightarrow \phi\ es\ un\ isomorfismo.$$

*Demostración*: Ver [SIL], Capítulo II, Corolario 2.4.1.

**Definición.** *Sea $\phi : C_1 \longrightarrow C_2$ una aplicación no constante de curvas lisas, y sea $P \in C_1$. El* **índice de ramificación de** *$\phi$* **en** *$P$ está dado por*

$$e_\phi(P) := ord_P(\phi^* t_{\phi(P)}),$$

*donde $t_{\phi(P)} \in K(C_2)$ es un parámetro uniformizante en $\phi(P)$. Se tiene que $e_\phi(P) \geq 1$, y se dice que $\phi$* **no ramifica en** *$P$ si $e_\phi(P) = 1$.*

**Proposición 2.4.7** *Sea $\phi : C_1 \longrightarrow C_2$ una aplicación no constante de curvas lisas. Entonces para todo $Q \in C_2$,*

$$deg(\phi) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P).$$

*Demostración*: Ver [SHA], Capítulo III, Sección 2, Teorema 1.

## 2.5 Divisores, diferenciales y el teorema de Riemann-Roch.

En esta sección "curva"querrá decir curva lisa.

### 2.5.1 Divisores.

**Definición.** *Sea $C$ una curva. El* **grupo de divisores de** *$C$, denotado por $Div(C)$, es el grupo abeliano libre generado por los puntos de $C$. Es decir, un* **divisor** *$D \in Div(C)$ es una suma formal*

$$D = \sum_{P \in C} n_P \cdot (P),$$

*con $n_P \in \mathbb{Z}$ y $n_P = 0$ para todo $P$ excepto un número finito. El* **grado de** *$D$ está definido por*

$$deg(D) = \sum_{P \in C} n_P.$$

*Si $C$ está definida sobre $K$, entonces $Gal(\overline{K}/K)$ actúa sobre $Div(C)$ de la forma siguiente:*

$$D^\sigma = \sum_{P \in C} n_P \cdot (P^\sigma) \quad con \;\; \sigma \in Gal(\overline{K}/K).$$

*Diremos que $D$ está* **definido sobre** *$K$ si $D^\sigma = D$, $\forall \sigma \in Gal(\overline{K}/K)$.*

**Definición.** *Sea $C$ una curva lisa, y sea $f \in \overline{K}(C)^*$. Asociamos a $f$ el* **divisor de** *$f$ definido como*

$$div(f) := \sum_{P \in C} ord_P(f) \cdot (P).$$

**Definición.** *Un divisor $D \in Div(C)$ es* **principal** *si $\exists\, f \in \overline{K}(C)^*$ tal que $div(f) = D$. Dados $D_1, D_2 \in Div(C)$, diremos que son* **linealmente equivalentes***, denotado por $D_1 \sim D_2$, si $D_1 - D_2$ es principal. El* **grupo de clases de divisores (o grupo de Picard) de** *$C$ está definido por el cociente*

$$Pic(C) := Div(C)/\sim$$

**Proposición 2.5.1** *Sea $C$ una curva lisa y $f \in \overline{K}(C)^*$. Entonces,*

$$deg(div(f)) = 0.$$

*Demostración*: Ver [HAR], Capítulo II, Corolario 6.4.

**Ejemplo 2.5.1** Sea $C$ la curva definida sobre $K$, con $car(K) \neq 2$, por

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3) \quad \text{con } e_1, e_2, e_3 \in K \text{ distintos.}$$

Vamos a hallar $div(x - e_i)$, $i = 1, 2, 3$ y $div(y)$. Tenemos que en $\mathbb{P}^2$, el homogeneizado de $x - e_i$ es $\dfrac{x - e_i z}{z}$.

Sea $P = [\alpha, \beta, 1]$ distinto de $P_i = [e_i, 0, 1]$ $i = 1, 2, 3$; entonces

$$ord_P\left(\frac{x - e_i z}{z}\right) = 0.$$

Para $P_i$, tenemos que $y$ es un parámetro en $P_i$. Además como $y^2 = \prod_{i=1}^{3}(x - e_i)$, entonces

$$(x - e_i) = y^2 \prod_{\substack{j = 1, 2, 3 \\ j \neq i}} (x - e_j)^{-1}.$$

Como $(x - e_j) \neq 0$ en $P_i$ tenemos:

$$ord_{P_i}\left(\frac{x - e_i z}{z}\right) = ord_{P_i}(x - e_i) = 2.$$

Ahora nos queda el punto $P_\infty = [0, 1, 0]$:

$$y^2 z = (x - e_1 z)(x - e_2 z)(x - e_3 z)$$

$$\frac{z}{y} = \left(\frac{x}{y} - e_1\frac{z}{y}\right)\left(\frac{x}{y} - e_2\frac{z}{y}\right)\left(\frac{x}{y} - e_3\frac{z}{y}\right).$$

Sabemos que la función $\frac{z}{y}$ tiene un cero en $P_\infty = [0, 1, 0]$ y por lo tanto, como $t = \frac{x}{y}$ es un parámetro en $P_\infty$, tenemos

$$\frac{z}{y} = t^3 f \text{ con } f \in \overline{K}[C]_\infty \text{ y } f(P_\infty) \neq 0. \tag{2.1}$$

Entonces

$$\frac{x - e_i z}{z} = \frac{\frac{x}{y} - e_i\frac{z}{y}}{\frac{z}{y}} = \frac{t - e_i t^3 f}{t^3 f} = \frac{1}{t^2} g$$

con $g \in \overline{K}[C]_{P_\infty}$ y $g(P_\infty) \neq 0$. Por lo tanto,

$$ord_{P_\infty}(x - e_i) = -2.$$

Entonces

$$\boxed{div(x - e_i) = 2(P_i) - 2(P_\infty)}$$

Calculemos finalmente $div(y)$. Se tiene que si $P = [\alpha, \beta, 1] \neq P_i$ $i = 1, 2, 3$ entonces

$$ord_P(y) = 0.$$

Además, como $y$ es un parámetro en $P_i$, se tiene que

$$ord_{P_i}(y) = 1.$$

Nos queda por ver $P_\infty = [0, 1, 0]$:

$$\frac{y}{z} = \left(\frac{z}{y}\right)^{-1} = t^{-3}f^{-1} = t^{-3}h,$$

con $h \in \overline{K}[C]_{P_\infty}$ y $h(P_\infty) \neq 0$. Entonces

$$ord_{P_\infty}(y) = -3.$$

Y podemos concluir que

$$\boxed{div(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty)}$$

### 2.5.2 Diferenciales.

**Definición.** *Sea $C$ una curva. El* **espacio de formas diferenciales meromorfas en** *$C$, denotado por $\Omega_C$, es el $\overline{K}(C)$-espacio vectorial generado por símbolos de la forma $dx$ para $x \in \overline{K}(C)$,cumpliendo las siguientes propiedades:*

*(i)* $d(x + y) = dx + dy, \quad \forall x, y \in \overline{K}(C).$

*(ii)* $d(xy) = ydx + xdy, \quad \forall x, y \in \overline{K}(C).$

*(iii)* $da = 0, \quad \forall a \in \overline{K}.$

Sea $\phi : C_1 \longrightarrow C_2$ una aplicación no constante entre curvas. Entonces la aplicación natural $\phi^* : \overline{K}(C_2) \longrightarrow \overline{K}(C_1)$ induce una aplicación entre espacios de formas diferenciales

$$\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}$$

$$\phi^* \left(\sum_i f_i dx_i\right) = \sum_i (\phi^* f_i) d(\phi^* x_i)$$

**Proposición 2.5.2** *Sea $C$ una curva. Entonces,*

*(i)* $dim_{\overline{K}(C)}\Omega_C = 1$

*(ii) Sea $x \in \overline{K}(C)$. El conjunto $\{dx\}$ es una $\overline{K}(C)$-base para $\Omega_C \iff \overline{K}(C)/\overline{K}(x)$ es una extensión finita y separable.*

*Demostración*:

(i) Se tiene que $\Omega_C$ es isomorfo al dual del espacio tangente a $C$. Por tanto, como $dim\, T_C = 1$, obtenemos $dim\, \Omega_C = 1$.

(ii) Si $\overline{K}(C)/\overline{K}(x)$ es una extensión finita y separable, entonces todo elemento $f \in \overline{K}(C)$ satisface una relación de la forma

$$F(f, x) = 0,$$

donde $F \in \overline{K}[T, x]$ es separable en $T$. Por tanto

$$\frac{\partial F}{\partial T}(f, x)df + \frac{\partial F}{\partial x}(f, x)dx = 0,$$

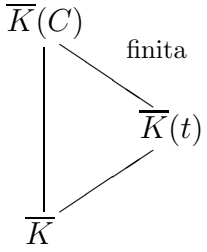
es decir,

$$df = -\frac{\frac{\partial F}{\partial x}(f, x)}{\frac{\partial F}{\partial T}(f, x)}dx.$$

Se tiene que $\dfrac{\partial F}{\partial T}(f, x) \neq 0$, ya que $F$ es separable en $T$. Y por lo tanto $dx$ es una $\overline{K}(C)$-base de $\Omega_C$.

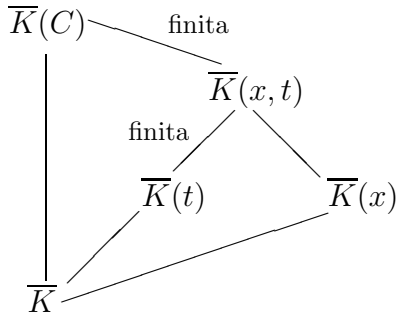
Ahora vamos a ver que si $dx$ es una $\overline{K}(C)$-base de $\Omega_C$ entonces $\overline{K}(C)/\overline{K}(x)$ es una extensión finita y separable.

(1) Finita:
Por ser $\overline{K}(C)$ cuerpo de funciones de una curva, su grado de trascendencia es 1, y por tanto se tiene la siguiente torre de extensiones




donde $t$ es una variable.

Queremos ver que la extensión $\overline{K}(C)/\overline{K}(x)$ es finita, para ello consideramos




Por ser la extensión $\overline{K}(x,t)/\overline{K}(t)$ finita, existe un polinomio con coeficientes en $\overline{K}$ tal que

$$\sum_{i,j} a_{ij}x^i t^j = 0,$$

es decir,

$$\sum_i \left( \sum_j a_{ij}t^j \right) x^i = 0.$$

Para algún $j \neq 0$ existe $i$ tal que $a_{ij} \neq 0$, ya que de lo contrario tendríamos que $x$ sería algebraico sobre $\overline{K}$; de modo que $x \in \overline{K}$ y $dx = 0$, pero esto es imposible por ser $dx$ base. Por tanto $t$ es raíz de un polinomio no nulo,

$$\sum_j \left( \sum_i a_{ij}x^i \right) t^j = 0,$$

con lo que $\overline{K}(x,t)/\overline{K}(x)$ es finita. Por tanto tenemos que $\overline{K}(C)/\overline{K}(x)$ es finita.

(2) Separable:
En primer lugar, si la extensión no es separable se tiene que $car(\overline{K}) = p > 0$.

Sea $f \in \overline{K}(C)$ no separable sobre $\overline{K}(x)$. Entonces existe un polinomio de la forma

$$F(x,T) = \sum_{i=0}^{d} q_i(x)T^{p \cdot i},$$

con $q_i(x) \in \overline{K}[x]$ tal que $(q_0, \ldots, q_d) = 1$, $F(x,f) = 0$ y tal que el grado de $F$ en $T$ es mínimo entre los polinomios para los que $f$ es una raíz ($F$ es el polinomio primitivo asociado al polinomio mínimo de $f$ sobre $\overline{K}(x)$). Tomamos derivadas y obtenemos

$$0 = d(F(x,f)) = \sum_{i=0}^{d} q_i'(x)f^{p \cdot i}dx.$$

Por tanto $\sum_{i=0}^{d} q_i'(x) f^{p\cdot i} = 0$, ya que $dx$ es una base. Sea

$$G(x,T) = \sum_{i=0}^{d} q_i'(x) T^{p\cdot i},$$

queremos ver $G = 0$. Supongamos lo contrario, entonces $G(x, f) = 0$ y por la definición de $F$ se tiene

$$G(x,T) = g(x) \cdot F(x,T)$$

con $g \in \overline{K}[x]$. Comparando los grados en $x$ observamos que esto es imposible. Por tanto $G = 0$, es decir, $q_i'(x) = 0$, de modo que $q_i(x) \in \overline{K}[x^p]$. Así obtenemos

$$F(x,T) = \sum_{i,j} a_{ij} x^{p\cdot j} T^{p\cdot j} = \left( \sum_{i,j} \sqrt[p]{a_{ij}}\, x^j T^i \right)^p,$$

en contradicción con la irreducibilidad de $F$.

□

**Proposición 2.5.3** *Sea $C$ una curva, $P \in C$ y sea $t \in \overline{K}(C)$ un parámetro uniformizante en $P$.*

*(i) Para todo $\omega \in \Omega_C$ existe una única función $g \in \overline{K}(C)$, dependiendo de $\omega$ y $t$, tal que*

$$\omega = g\,dt.$$

*(ii) Sea $f \in \overline{K}(C)$ regular en $P$. Entonces $\dfrac{df}{dt}$ es también regular en $P$.*

*(iii) Si definimos el* **orden de $\omega$ en $P$** *como*

$$ord_P(\omega) := ord_P(g),$$

*se tiene que sólo depende de $\omega$ y $P$, es decir, es independiente de la elección del parámetro uniformizante $t$.*

*(iv) Para todo $P \in C$, salvo un número finito,*

$$ord_P(\omega) = 0.$$

*Demostración*:

(i) Usando la proposición 2.4.2 tenemos que $t$ está en las condiciones de aplicar la proposición 2.5.2 y por lo tanto $dt$ es una $\overline{K}(C)$-base de $\Omega_C$.

(ii) Ver [ROB], Capítulo II, Proposición 3.10.

(iii) Sea $t'$ otro parámetro uniformizante en $P$. Entonces por $(ii)$, $dt/dt'$ y $dt'/dt$ son ambas regulares en $P$, entonces $ord_P(dt'/dt) = 0$. Como

$$\omega = gdt' = g\left(\frac{dt'}{dt}\right)dt,$$

se obtiene el resultado deseado.

(iv) Sea $x \in \overline{K}(C)$ tal que $\overline{K}(C)/\overline{K}(x)$ es separable, y escribimos $\omega = fdx$. Por la Proposición 2.2,a del Capítulo IV de [HAR], la aplicación $x : C \longrightarrow \mathbb{P}^1$ ramifica en un número finito de puntos de $C$. Entonces descartando a un número finito de puntos, podemos restringirnos a puntos $P \in C$ tal que $f(P) \neq 0, \infty, x(P) \neq \infty$, y $x : C \longrightarrow \mathbb{P}^1$ no ramifica en $P$. Pero las dos últimas condiciones implican que $x - x(P)$ es un parámetro uniformizante en $P$, y por tanto

$$ord_P(\omega) = ord_P(fd(x - x(P)) = 0.$$

□

Al igual que asociamos un divisor a toda función $f \in \overline{K}(C)^*$, vamos a asociar un divisor a toda forma diferencial $\omega \in \Omega_C$.

**Definición.** *Sea $\omega \in \Omega_C$. El* **divisor asociado a** $\omega$ *es*

$$div(\omega) := \sum_{P \in C} ord_P(\omega) \cdot (P) \in Div(C).$$

**Definición.** *Una diferencial $\omega \in \Omega_C$ se dice que es* **regular** *(u* **holomorfa***) si*

$$ord_P(\omega) \geq 0 \quad \forall P \in C.$$

*Y es* **no nula** *si*

$$ord_P(\omega) \leq 0 \quad \forall P \in C.$$

Si $\omega_1, \omega_2 \in \Omega_C$ son diferenciales distintas de cero, entonces la proposición 2.5.3 nos dice que existe una función $f \in \overline{K}(C)^*$ tal que

$$\omega_1 = f\omega_2,$$

de donde

$$div(\omega_1) = div(f) + div(\omega_2).$$

Esto nos muestra que la siguiente definición tiene sentido.

**Definición.** *La* **clase del divisor canónico de** $C$ *es la imagen en $Pic(C)$ de $div(\omega)$, con $\omega \in \Omega_C$ distinta de cero. Cualquier divisor en la clase del divisor canónico es llamado* **divisor canónico**.

**Ejemplo 2.5.2** Vamos a ver que no hay diferenciales holomorfas en $\mathbb{P}^1$.

Sea $t$ una función coordenada en $\mathbb{P}^1$. Veamos cómo es $div(dt)$. Para todo $\alpha \in K$, $t-\alpha$ es un parámetro uniformizante en $\alpha := [\alpha, 1]$, por lo que

$$ord_\alpha(dt) = ord_\alpha(d(t-\alpha)) = 0.$$

En $\infty := [1,0] \in \mathbb{P}^1$, el parámetro uniformizante es $\dfrac{1}{t}$, por lo tanto

$$ord_\infty(dt) = ord_\infty\left(-t^2 d\left(\frac{1}{t}\right)\right) = -2.$$

Hemos obtenido:

$$div(dt) = -2(P_\infty) \Longrightarrow \ dt \text{ no es holomorfa.} \tag{2.2}$$

Sea $\omega \in \Omega^1_{\mathbb{P}}$ distinta de cero; por la proposición 2.5.3,

$$\omega = f dt \text{ para alguna } f \in \overline{K}(C)^*.$$

El divisor asociado a $\omega$ es $div(\omega) = div(f) + div(dt)$, cuyo grado es

$$deg(div(\omega)) = deg(div(f)) + deg(div(dt)) = deg(div(dt)) = -2 \tag{2.3}$$

por la proposición 2.5.1 y por (2.2).

Sea $\omega$ una diferencial holomorfa en $\mathbb{P}^1$ entonces

$$ord_P(\omega) \geq 0 \quad \forall P \in \mathbb{P}^1.$$

Si consideramos el grado del divisor asociado a $\omega$ tenemos

$$deg(div(\omega)) \geq 0$$

en contradicción con (2.3). Por lo tanto no existen diferenciales holomorfas en $\mathbb{P}^1$.

**Ejemplo 2.5.3** Sea $C$ la curva definida por

$$C : y^2 = (x-e_1)(x-e_2)(x-e_3)$$

con $e_1, e_2, e_3 \in \overline{K}$ distintos y $car(K) \neq 2$.

Vamos a hallar $div(dx)$. Sea $P = [\alpha, \beta, 1]$ distinto de $P_i = [e_i, 0, 1]$ $i = 1, 2, 3$. Entonces $x - \alpha$ es un parámetro uniformizante en $P$ y como $dx = d(x-\alpha)$ se tiene

$$ord_P(dx) = ord_P(d(x-\alpha)) = 0.$$

Sea $P_i = [e_i, 0, 1]$; entonces $y$ es un parámetro uniformizante en $P_i$. Ahora

$$y^2 = (x-e_1)(x-e_2)(x-e_3) = f(x),$$

luego

$$2ydy = f'(x)dx \Longrightarrow dx = \frac{2}{f'(x)}ydy.$$

$P_i$ es un punto no singular de $C$, así que $f'(e_i) \neq 0$. Por lo tanto,

$$ord_{P_i}(dx) = 1.$$

Ahora estudiamos lo que sucede en $P_\infty = [0, 1, 0]$. Tenemos

$$dx = d\left(\frac{x}{z}\right) = d\left(\frac{x/y}{z/y}\right) = \frac{\frac{z}{y}d\left(\frac{x}{y}\right) - \frac{x}{y}d\left(\frac{z}{y}\right)}{(z/y)^2}.$$

Un parámetro uniformizante en $P_\infty$ es $t = \frac{x}{y}$ y vimos en el ejemplo 2.5.1 que

$$\frac{z}{y} = t^3 f \text{ con } f \in \overline{K}[C]_{P_\infty} \text{ y } f(P_\infty) \neq 0.$$

Por lo tanto,

$$d\left(\frac{x}{z}\right) = \frac{t^3(-2f - tf')dt}{t^6 f^2} = t^{-3}ldt,$$

con $l \in \overline{K}[C]_{P_\infty}$ y $l(P_\infty) \neq 0$. Entonces

$$ord_{P_\infty}(dx) = -3.$$

Hemos obtenido

$$\boxed{div(dx) = (P_1) + (P_2) + (P_3) - 3(P_\infty)}$$

Vimos en el ejemplo 2.5.1 que

$$div(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

Por lo tanto si tomamos la diferencial $dx/y$ obtenemos

$$\boxed{div(dx/y) = 0}$$

Luego $dx/y$ es una diferencial holomorfa en $C$ y además no se anula.

### 2.5.3 Teorema de Riemann-Roch.

Vamos a introducir un orden parcial en el grupo de divisores de una curva.

**Definición.** *Un divisor* $D = \sum_{P \in C} n_P \cdot (P) \in Div(C)$ *es* **positivo** *(o* **efectivo***) si* $n_P \geq 0 \quad \forall P \in C$. *Lo denoteremos por* $D \geq 0$. *Si* $D_1, D_2 \in Div(C)$, *escribiremos* $D_1 \geq D_2$ *para indicar que el divisor* $D_1 - D_2$ *es positivo.*

**Definición.** *Sea* $D \in Div(C)$. *Asociamos a* $D$ *el siguiente conjunto de funciones*

$$\mathcal{L}(D) := \{f \in \overline{K}(C)^* : div(f) + D \geq 0\} \cup \{0\}.$$

**Proposición 2.5.4** *Sea $D \in Div(C)$.*

*(i) $\mathcal{L}(D)$ es un $\overline{K}$-espacio vectorial de dimensión finita, lo denotaremos por*

$$\ell(D) := dim_{\overline{K}}\mathcal{L}(D).$$

*(ii) Si $deg(D) < 0$ entonces*

$$\mathcal{L}(D) = \{0\} \quad y \quad \ell(D) = 0.$$

*(iii) Si $D' \in Div(C)$ es linealmente equivalente a $D$, entonces*

$$\mathcal{L}(D) \simeq \mathcal{L}(D')$$

*y por lo tanto*

$$\ell(D) = \ell(D').$$

*Demostración*:

(i) Ver [HAR], Capítulo II, Teorema 5.19.

(ii) Sea $f \in \mathcal{L}(D)$ no idénticamente cero. Entonces

$$div(f) \geq -D.$$

Tomando grados y utilizando la proposición 2.5.1 obtenemos la siguiente contradicción

$$0 = deg(div(f)) \geq deg(-D) = -deg(D) > 0.$$

(iii) Si $D' = D + div(g)$ con $g \in \overline{K}(C)^*$, entonces la aplicación

$$\begin{array}{ccc} \mathcal{L}(D) & \longrightarrow & \mathcal{L}(D') \\ f & \mapsto & f \cdot g \end{array}$$

es un isomorfismo.

□

**Observación 2.5.5** Sea $K_C \in Div(C)$ un divisor canónico de $C$, digamos

$$K_C = div(\omega).$$

Entonces cada función $f$ tiene la propiedad

$$f \in \mathcal{L}(K_C) \Longleftrightarrow div(f) + div(\omega) \geq 0 \Longleftrightarrow div(f\omega) \geq 0 \Longleftrightarrow f\omega \text{ es holomorfa.}$$

Sabemos que toda diferencial de $C$ tiene la forma $f\omega$ para alguna función $f \in \overline{K}(C)^*$ y por lo tanto podemos establecer un isomorfismo de $\overline{K}$-espacios vectoriales :

$$\mathcal{L}(K_C) \simeq \{\omega \in \Omega_C : \omega \text{ es holomorfa }\}. \tag{2.4}$$

La dimensión de $\mathcal{L}(K_C)$, $\ell(K_C)$, es un importante invariante de la curva $C$.

Ahora vamos a ver un teorema central en Geometría Algebraica.

**Teorema de Riemann-Roch.** *Sea $C$ una curva lisa y $K_C$ un divisor canónico de $C$. Existe un entero $g := g(C) \geq 0$, llamado* **género de** *$C$, tal que para todo divisor $D \in Div(C)$*

$$\boxed{\ell(D) - \ell(K_C - D) = deg(D) - g + 1.}$$

*Demostración*: Ver cualquier libro de Geometría Algebraica básica, en particular [HAR], Capítulo IV, Teorema 1.3.

**Corolario.**

*(i)* $\ell(K_C) = g$.

*(ii)* $deg(K_C) = 2g - 2$.

*(iii) Si* $deg(D) > 2g - 2$, *entonces* $\ell(D) = deg(D) - g + 1$.

*Demostración*:

(i) Aplicando el teorema de Riemann-Roch al divisor $D = 0$ y observando que $\mathcal{L}(D) = \mathcal{L}(0) = \overline{K}$ se obtiene $\ell(D) = \ell(0) = 1$. Por lo tanto,

$$\ell(0) - \ell(K_C) = deg(D) - g + 1 \Longrightarrow \ell(K_C) = g.$$

(ii) Aplicamos el teorema de Riemann-Roch al divisor $D = K_C$ y utilizando $(i)$ obtenemos

$$\ell(K_C) - \ell(0) = deg(K_C) - g + 1 \Longrightarrow deg(K_C) = 2g - 2.$$

(iii) Se tiene por hipótesis y por $(ii)$ que $deg(K_C - D) = deg(K_C) - deg(D) < 0$. Utilizando la proposición 2.5.4 obtenemos

$$\ell(K_C - D) = 0;$$

y aplicando el teorema de Riemann-Roch

$$\ell(D) = deg(D) - g + 1.$$

□

**Ejemplo 2.5.4** Sea $C = \mathbb{P}^1$. Vimos en la ejemplo 2.5.2 que $\mathbb{P}^1$ no tenía diferenciales holomorfas. Usando (2.4) obtenemos

$$\boxed{g(\mathbb{P}^1) = 0}.$$

**Ejemplo 2.5.5** Vimos en el ejemplo 2.5.3 que si tenemos la curva $C$ dada por

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

con $e_1, e_2, e_3 \in \overline{K}$ distintos y $car(K) \neq 2$, entonces $dx/y$ es una diferencial holomorfa de $C$ que no se anula y que cumple

$$div(dx/y) = 0.$$

Por lo tanto si tomamos $K_C = div(dx/y)$ obtenemos, utilizando el apartado $(ii)$ del corolario del teorema de Riemann-Roch, el siguiente resultado

$$0 = deg(0) = deg(K_C) = 2g - 2.$$

Por tanto,

$$\boxed{g(C) = 1}.$$

**Proposición 2.5.6** *Sea $C/K$ una curva lisa, y sea $D$ un divisor definido sobre $K$. Entonces $\mathcal{L}(D)$ tiene una base formada por funciones de $K(C)$.*

*Demostración*: Ver [SIL], Capítulo II, Proposición 5.8.

Enunciaremos finalmente otro teorema fundamental junto con el teorema de Riemann-Roch, que nos relaciona el género de dos curvas.

**Teorema de Hurwitz.** *Sea $\phi : C_1 \longrightarrow C_2$ una aplicación separable no constante de curvas lisas. Entonces*

$$2g(C_1) - 2 \geq deg(\phi)(2g(C_2) - 2) + \sum_{P \in C_1} (e_\phi(P) - 1),$$

*donde $g(C_i)$ es el género de $C_i$. Además la igualdad ocurre en lo siguientes casos:*

*(i)* $car(K) = 0$.

*(ii)* $car(K) = p > 0$ *y* $p$ *no divide a* $e_\phi(P)$ $\forall P \in C_1$.

*Demostración*: Ver [SIL], Capítulo II, Teorema 5.9.

## 2.6 Curvas elípticas.

**Definición.** *Una* **curva elíptica** *es un par $(E, \mathcal{O})$, donde $E$ es una curva lisa de género 1 y $\mathcal{O} \in E$. La curva elíptica $(E, \mathcal{O})$ está* **definida sobre** *$K$ si $E$ está definida sobre $K$ y $\mathcal{O} \in E(K)$.*

Vamos a ver que la definición dada en el capítulo 1 de curva elíptica es equivalente a ésta. Para ello vamos a ver el siguiente teorema que es una aplicación del teorema de Riemann-Roch.

**Teorema 2.6.1** *Sea $E$ una curva elíptica definida sobre un cuerpo $K$. Entonces*

*(i) Existen funciones $x, y \in K(E)$ tales que la función*

$$\begin{aligned} \phi : E &\longrightarrow \mathbb{P}^2 \\ \phi &= [x, y, 1] \end{aligned}$$

*es un isomorfismo de $E/K$ en una curva $C$ dada por la ecuación de Weierstrass*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

*con $a_1, a_2, a_3, a_4, a_6 \in K$. Además $\phi(\mathcal{O}) = [0, 1, 0]$. ($x, y$ se denominan* **funciones coordenadas de Weierstrass de** *$E$).*

*(ii) Dos ecuaciones de Weierstrass para $E$ están relacionadas por un cambio de variable de la forma*

$$\begin{cases} x = u^2x' + r, \\ y = u^3y' + su^2x' + t, \end{cases}$$

*con $u, r, s, t \in K$, $u \neq 0$.*

*(iii) Recíprocamente, cualquier curva lisa $C$ dada por una ecuación de Weierstrass es isomorfa a una curva elíptica definida sobre $K$ con elemento neutro $\mathcal{O} = [0, 1, 0]$.*

*Demostración*:

(i) Consideremos los espacios $\mathcal{L}(n\mathcal{O})$ $n = 1, 2, \ldots$, y observamos que $\mathcal{L}(n\mathcal{O}) \subset \mathcal{L}((n+1)\mathcal{O})$. Usando el apartado (*iii*) del corolario del teorema de Riemann-Roch en nuestra curva, que tiene género 1, tenemos:

$$\text{Si } deg(D) > 0 \Longrightarrow \ell(D) = deg(D).$$

Entonces,

$$\ell(n\mathcal{O}) = n.$$

Por la proposición 2.5.6 podemos elegir funciones de $K(E)$ que formen una base de $\mathcal{L}(n\mathcal{O})$.

- $\ell(\mathcal{O}) = 1$. $\mathcal{L}(\mathcal{O}) \cong \overline{K}$, entonces $1 \in \overline{K}$ es una base de $\mathcal{L}(\mathcal{O})$.
- $\ell(2\mathcal{O}) = 2$. Como $\mathcal{L}(\mathcal{O}) \subsetneq \mathcal{L}(2\mathcal{O})$ tomamos $x \in K(E)$ de tal forma que $x$ tenga un polo doble en $\mathcal{O}$. Una base de $\mathcal{L}(2\mathcal{O})$ es $\{1, x\}$.
- $\ell(3\mathcal{O}) = 3$. Como $\mathcal{L}(2\mathcal{O}) \subsetneq \mathcal{L}(3\mathcal{O})$ escogemos $y \in K(E)$ con un polo triple en $\mathcal{O}$. Una base de $\mathcal{L}(3\mathcal{O})$ es $\{1, x, y\}$.
- $\ell(4\mathcal{O}) = 4$. Podemos tomar $\{1, x, y, x^2\}$ como base de $\mathcal{L}(4\mathcal{O})$, ya que $x^2$ tiene un polo de orden 4 en $\mathcal{O}$ y $x^2 \notin \mathcal{L}(3\mathcal{O})$.
- $\ell(5\mathcal{O}) = 5$. Cogemos como base $\{1, x, y, x^2, xy\}$, ya que $xy$ tiene un polo de orden 5 en $\mathcal{O}$ y $xy \notin \mathcal{L}(4\mathcal{O})$.

– $\ell(6\mathcal{O}) = 6$ y $\{1, x, y, x^2, xy, x^3, y^2\} \subset \mathcal{L}(6\mathcal{O})$, por lo tanto debe haber una relación lineal

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6x^3 + A_7y^2 = 0,$$

con $A_i$ no todos iguales a cero. Además por la proposición 2.5.6 se tiene que $A_i \in K$ $i = 1, \ldots, 7$.
Además $A_6 \cdot A_7 \neq 0$, ya que de lo contrario $1, x, y, xy, x^2$ serían linealmente dependientes.

Por lo tanto podemos hacer el siguiente cambio

$$\begin{cases} x = -A_6A_7x', \\ y = A_6A_7^2y', \end{cases}$$

y después dividiendo por ${A_6}^3{A_7}^4$, obtenemos una ecuación cúbica en la forma de Weierstrass. Esto nos da la aplicación deseada,

$$\begin{array}{c} \phi : E \longrightarrow \mathbb{P}^2 \\ \phi = [x, y, 1], \end{array}$$

cuya imagen cae en la curva $C$ descrita por la ecuación de Weierstrass anterior.

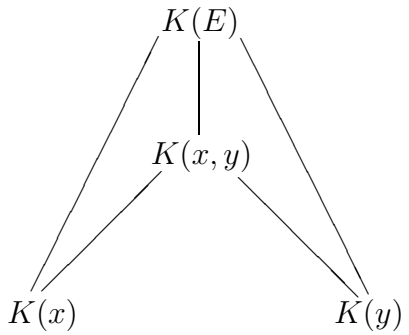
Tenemos que $\phi$ es una aplicación racional y $E$ es lisa. Entonces, por la proposición 2.4.3, $\phi$ es un morfismo. Ahora utilizando el teorema 2.4.4 aplicado a $\phi : E \to C \subset \mathbb{P}^2$, que es claramente no constante, obtenemos que es sobreyectiva.

El siguiente paso es mostrar que la aplicación $\phi : E \longrightarrow C \subset \mathbb{P}^2$ tiene grado 1, o equivalentemente que $K(E) = K(x, y)$. Consideramos las aplicaciones

$$\begin{array}{rcl} \phi_1 : & E \longrightarrow \mathbb{P}^1 \\ & \phi_1 = [x, 1] \end{array} \quad \text{y} \quad \begin{array}{rcl} \phi_2 : & E \longrightarrow \mathbb{P}^1 \\ & \phi_2 = [y, 1] \end{array}$$

Como $x$ tiene un polo de orden 2 en $\mathcal{O}$ y no tiene ningún otro polo, la proposición 2.4.7 aplicada al punto $Q = [1, 0]$, nos da $deg(\phi_1) = 2$.
Ahora como $y$ tiene un polo de orden 3 en $\mathcal{O}$, aplicando de nuevo la proposición 2.4.7, tenemos $deg(\phi_2) = 3$.

Utilizando la siguiente torre de cuerpos




tenemos que

$$[K(E) : K(x)] = deg(\phi_1) = 2 \quad \text{y} \quad [K(E) : K(y)] = deg(\phi_2) = 3.$$

Por lo tanto, $[K(E) : K(x, y)]$ divide a 2 y a 3, así que

$$[K(E) : K(x, y)] = 1.$$

Esto es, $K(E) = K(x, y)$.

Ahora veamos que $C$ es lisa, y para ello supondremos que $C$ no es lisa y llegaremos a una contradicción. Si $C$ es singular la proposición 1.5.6 nos dice que existe una aplicación $\varphi : C \longrightarrow \mathbb{P}^1$ de grado 1. Entonces la composición $\varphi \circ \phi : E \longrightarrow \mathbb{P}^1$ es una aplicación de grado 1 entre curvas lisas; la proposición 2.4.6 nos dice que es un isomorfismo. Esto contradice el hecho de que $E$ tiene género 1 y $\mathbb{P}^1$ tiene género 0. Por lo tanto $C$ es lisa. Y utilizando de nuevo la proposición 2.4.6 tenemos que $E$ es isomorfa a $C$, ya que tenemos un morfismo de curvas lisas $E$ y $C$ de grado 1.

(ii) Sean $\{x, y\}$ y $\{x', y'\}$ dos conjuntos de funciones coordenadas de Weierstrass en $E$. Entonces $x$ y $x'$ tienen polos de orden 2 en $\mathcal{O}$. Por lo tanto $\{1, x\}$ e $\{1, x'\}$ son base de $\mathcal{L}(2\mathcal{O})$ y

$$x = u_1 x' + r \quad u_1, r \in K \quad u_1 \neq 0.$$

Análogamente, $y$ e $y'$ tienen polos de orden 3 en $\mathcal{O}$ , $\{1, x, y\}$ y $\{1, x', y'\}$ son base de $\mathcal{L}(3\mathcal{O})$, luego

$$y = u_2 y' + s_2 x' + t \quad u_2, s_2, t \in K \quad u_2 \neq 0.$$

Además $(x, y)$ y $(x', y')$ satisfacen la ecuación de Weierstrass en la que los coeficientes de $x^3$ e $y^2$ son 1; por lo tanto ${u_1}^3 = {u_2}^2$. Poniendo

$$u = \frac{u_2}{u_1} \quad \text{y} \quad s = \frac{s_2}{u^2},$$

obtenemos que el cambio de variables es de la forma

$$\begin{cases} X = u^2 X' + r, \\ Y = u^3 Y' + s u^2 X' + t, \end{cases}$$

(iii) Supongamos[1] que $car(K) \neq 2$. Sea $E$ una curva lisa dada por una ecuación de Weierstrass. En la sección §1.5 vimos que si teníamos $car(K) \neq 2$ entonces nuestra curva se podía poner en la forma

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \quad \text{con } e_1, e_2, e_3 \in \overline{K} \text{ distintos.}$$

Vimos en el ejemplo 2.5.5 que entonces

$$g(E) = 1,$$

y junto con el punto $\mathcal{O} \in E$ , tenemos que $(E, \mathcal{O})$ es una curva elíptica.

□

[1]Para ver el caso en que $car(K) = 2$ ver [SIL], Capítulo III, Proposición 3.1,c.

# Capítulo 3

# Teorema de Mordell.

En este capítulo demostraremos el siguiente teorema:

**Teorema de Mordell.** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$. Entonces $E(\mathbb{Q})$ es un grupo abeliano finitamente generado.*

La demostración de este teorema consistirá en la aplicación del llamado Teorema del descenso, que veremos en la sección §1. Dicho teorema nos asegura que si en un grupo abeliano $A$ hay definida una función altura que cumple unas determinadas hipótesis y si existe un entero $m \geq 2$ de tal forma que $A/mA$ es finito, entonces $A$ está finitamente generado.

En la sección §2 demostraremos el Teorema Débil de Mordell, que nos asegura que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.

En la sección §3 definiremos una función altura en el grupo abeliano $E(\mathbb{Q})$, de tal forma que aplicando el Teorema del Descenso junto al Teorema Débil de Mordell, tendremos demostrado el Teorema de Mordell.

Así, el Teorema de Mordell nos dice que

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r,$$

donde $E(\mathbb{Q})_{tors}$ es el **subgrupo de torsión de** $E(\mathbb{Q})$ y $r$ es el **rango de** $E(\mathbb{Q})$.

Para una curva elíptica definida sobre $\mathbb{Q}$ es posible calcular completamente la estructura de $E(\mathbb{Q})_{tors}$, como veremos en el capítulo 4. Sin embargo, el rango es mucho más dificil de calcular y en general no se conocen métodos que nos garanticen cómo hallar el rango de una curva elíptica dada. Trataremos el rango en los últimos capítulos de este trabajo.

Por último, en la sección §4 enunciaremos varias generalizaciones del Teorema de Mordell.

## 3.1 El método del descenso.

**Teorema del descenso.** *Sea $A$ un grupo abeliano y sea $h : A \longrightarrow \mathbb{R}$ una función "altura "con las siguientes tres propiedades:*

*(i) Dado $Q \in A$, existe una constante $C_1 = C_1(Q)$ que depende de $Q$ y $A$, tal que para todo $P \in A$,*

$$h(P \oplus Q) \leq 2h(P) + C_1.$$

*(ii) Existe un entero $m \geq 2$ y una constante $C_2$ que depende sólo de $A$, tal que para todo $P \in A$,*

$$h([m]P) \geq m^2 h(P) - C_2.$$

*(iii) Para cualquier constante $C_3$,*

$$\{P \in A : h(P) \leq C_3\} \text{ es un conjunto finito.}$$

*Si suponemos además que para el entero $m$ en $(ii)$, el grupo cociente $A/mA$ es finito, entonces $A$ está finitamente generado.*

*Demostración*: Elegimos $Q_1, \ldots, Q_r \in A$, representantes de las clases de $A/mA$. Por ser $A/mA$ finito sabemos que es un conjunto finito. Si consideramos un $P \in A$, existirá $i$ tal que $P - Q_i \in mA$, es decir,

$$\exists i_1 \in \{1, \ldots, r\} \text{ y } \exists P_1 \in A \text{ tal que } P - Q_{i_1} = [m]P_1.$$

Continuando el proceso obtenemos sucesivamente:

$$\begin{aligned} P_1 &= [m]P_2 + Q_{i_2}, \\ &\vdots \\ P_{n-1} &= [m]P_n + Q_{i_n}. \end{aligned}$$

Por lo que podemos escribir

$$\begin{aligned} P &= Q_{i_1} + [m]P_1 = Q_{i_1} + [m]Q_{i_2} + [m^2]P_2 = \ldots = \\ &= [m^n]P_n + \sum_{j=1}^{n} [m^{j-1}]Q_{i_j}. \end{aligned}$$

Es decir,

$$P \in < Q_1, \ldots, Q_r, P_n > .$$

Si demostramos que existe una constante $C$ independiente del punto $P$ tal que $h(P_n) \leq C$ para un cierto $n$, habremos acabado, ya que tendremos que $A$ está generado por $\{Q_1, \ldots, Q_r\} \cup \{P \in A : h(P) \leq C\}$; y este conjunto es finito por la propiedad $(iii)$ de $h$. Vamos a buscar dicha contante. Para cada $j$, tenemos por $(ii)$ que

$$h([m]P_j) \geq m^2 h(P_j) - C_2,$$

así que

$$h(P_j) \leq \frac{1}{m^2}[h([m]P_j) + C_2] = \frac{1}{m^2}[h(P_{j-1} \ominus Q_{i_j}) + C_2].$$

Y por $(i)$ obtenemos

$$h(P_j) \leq \frac{1}{m^2}[2h(P_{j-1}) + C_1' + C_2], \tag{3.1}$$

donde $C_1' = \max\limits_{1\leq i\leq r}\{C_1(\ominus Q_i)\}$. Además $C_1'$ y $C_2$ no dependen de $P_j$. Ahora usamos la desigualdad (3.1) repetidamente, empezando por $P_n$ y llegando a $P$. Así obtenemos:

$$\begin{aligned}
h(P_n) &\leq \frac{1}{m^2}[2h(P_{n-1}) + C_1' + C_2] = \\
&= \frac{2}{m^2}h(P_{n-1}) + \frac{1}{m^2}[C_1' + C_2] \leq \\
&\leq \frac{2}{m^2}\left[\frac{1}{m^2}[2h(P_{n-2}) + C_1' + C_2]\right] + \frac{1}{m^2}[C_1' + C_2] = \\
&= \left(\frac{2}{m^2}\right)^2 h(P_{n-2}) + \left[\frac{1}{m^2} + \frac{2}{m^4}\right][C_1' + C_2] \leq \dots \\
&\vdots \qquad\qquad\qquad \vdots \\
&\leq \left(\frac{2}{m^2}\right)^n h(P) + \left[\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \dots \frac{2^{n-1}}{m^{2n}}\right][C_1' + C_2] \leq \\
&\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{2}[C_1' + C_2] \cdot \sum_{i=1}^{n-1}\left(\frac{2}{m^2}\right)^i.
\end{aligned}$$

Y usando que $m \geq 2$ obtenemos

$$\begin{aligned}
h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1' + C_2}{2} \cdot \frac{\frac{2}{m^2}}{1 - \frac{2}{m^2}} \leq \\
&\leq 2^{-n}h(P) + \frac{C_1' + C_2}{2}.
\end{aligned}$$

Se sigue que tomando un $n$ suficientemente grande, se cumplirá que

$$h(P_n) \leq 1 + \frac{C_1' + C_2}{2},$$

y por tanto todo elemento de $A$ es una combinación lineal de puntos del conjunto

$$\{Q_1, \dots, Q_r\} \cup \left\{Q \in A : h(Q) \leq 1 + \frac{C_1' + C_2}{2}\right\},$$

que es un conjunto finito por la propiedad $(iii)$. Esto prueba que $A$ está finitamente generado.

□

Una pregunta que nos podemos hacer, a la vista de la demostración del teorema del descenso, es cómo encontrar generadores para $A$. Primero tendremos que ser capaces de calcular las constantes $C_1 := C_1(Q_i)$, para cada elemento $Q_1, \ldots, Q_r \in A$, los representantes de las clases de $A/mA$. Luego tendremos que ser capaces de calcular la constante $C_2$. Y, por último para cualquier constante $C_3$, deberemos ser capaces de encontrar los elementos en el conjunto finito $\{P \in A : h(P) \leq C_3\}$.

Se pueden obtener estas constantes para las funciones altura, que definirenos para curvas elípticas, con tal de que podamos encontrar elementos de $E(K)$ que generen el grupo finito $E(K)/mE(K)$ (Ver [SIL], Ej. 8.18). Desafortunadamente, no se conoce ningún método que nos proprocione generadores para $E(K)/mE(K)$.

## 3.2 Teorema débil de Mordell.

**Teorema débil de Mordell.** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$. Entonces el grupo abeliano $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.*

Antes de la demostración veremos algunos resultados que nos serán necesarios.

**Proposición 3.2.1** *Sea $E$ una curva eliptica definida sobre $\mathbb{Q}$ por una ecuación de Weierstrass de la forma*

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

*El polinomio $f(x)$ se factoriza como:*

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma).$$

*Sea $K$ el cuerpo de descomposición de $f(x) = (x - \alpha)(x - \beta)(x - \gamma)$, y*

$$E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\phi} E(K)/2E(K)$$

*el homomorfismo canónico. Entonces,*

$$|\ker \phi| \leq 2^{2[K:\mathbb{Q}]}\ .$$

*Demostración*: Si $P = (x, y)$ es un elemento de $E(K)$ y $\sigma \in Gal(K/\mathbb{Q})$, entonces

$$P^\sigma = (\sigma(x), \sigma(y)) \in E(K).$$

Además $\sigma$ actua sobre $E(K)$ como un homomorfismo de grupos, esto es,

$$(P \oplus Q)^\sigma = P^\sigma \oplus Q^\sigma,$$

ya que $E$ está definida sobre $\mathbb{Q}$.

Definiremos ahora

$$E[2] := \{Q \in E(K) : [2]Q = \mathcal{O}\}.$$

Para cada $P \in \ker \phi$, elegimos $Q_P \in E(K)$ de manera que $[2]Q_P = P$. Entonces obtenemos una aplicación:

$$\begin{array}{rccc} \lambda_P : & Gal(K/\mathbb{Q}) & \longrightarrow & E[2] \\ & \sigma & \longmapsto & \lambda_P(\sigma) := Q_P^\sigma \ominus Q_P. \end{array}$$

Veamos que se tiene que $\lambda_P(\sigma) \in E[2]$ para todo $\sigma \in Gal(K/\mathbb{Q})$:

$$\begin{array}{rcl} [2]\lambda_P(\sigma) & = & [2](Q_P^\sigma \ominus Q_P) = ([2]Q_P)^\sigma \ominus [2]Q_P = \\ & = & P^\sigma \ominus P = \mathcal{O}, \end{array}$$

ya que como $P \in E(\mathbb{Q})$, $P^\sigma = P$. Si $\lambda_P = \lambda_{P'}$, entonces

$$Q_P^\sigma \ominus Q_P = \lambda_P(\sigma) = \lambda_{P'}(\sigma) = Q_{P'}^\sigma \ominus Q_{P'} \quad \forall \sigma \in Gal(K/\mathbb{Q}).$$

Por tanto,

$$(Q_P \ominus Q_{P'})^\sigma = Q_P^\sigma \ominus Q_{P'}^\sigma = Q_P \ominus Q_{P'} \qquad \forall \sigma \in Gal(K/\mathbb{Q}),$$

y como $K$ es una extensión normal de $\mathbb{Q}$, se tiene que $K^{Gal(K/\mathbb{Q})} = \mathbb{Q}$ (es decir, los elementos de $K$ que son invariantes bajo la acción de todo el grupo $Gal(K/\mathbb{Q})$, son los elementos de $\mathbb{Q}$). Por tanto,

$$Q_P \ominus Q_{P'} \in E(\mathbb{Q}).$$

Así pues, si $\lambda_P = \lambda_{P'}$, se tiene $P' - P = [2](Q_{P'} - Q_P) \in 2E(\mathbb{Q})$. Tenemos por tanto una aplicación inyectiva

$$\lambda : \ker \phi \longrightarrow Aplicaciones(Gal(K/\mathbb{Q}), E[2]),$$

de modo que

$$|\ker \phi| \leq \#Aplicaciones(Gal(K/\mathbb{Q}), E[2]).$$

Ahora, utilizando el teorema fundamental de la teoría de Galois tenemos que

$$\#Aplicaciones(Gal(K/\mathbb{Q}), E[2]) = 4^{|Gal(K/\mathbb{Q})|} = 4^{[K:\mathbb{Q}]},$$

y obtenemos el resultado deseado.

□

**Corolario.**

$$|E(K)/2E(K)| < \infty \Longrightarrow |E(\mathbb{Q})/2E(\mathbb{Q})| < \infty.$$

Por tanto, para ver que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito, basta con ver que $E(K)/2E(K)$ es finito.

En lo que sigue, denotaremos:

$K^*$ el grupo multiplicativo.

$K^{*2} = \{k \in K^* : \exists k' \in K^* \text{ tal que } k = (k')^2\}$.

$E$ una curva elíptica dada por $y^2 = (x-\alpha)(x-\beta)(x-\gamma) = f(x)$, con $K$ el cuerpo de descomposición de $f(x)$.

**Proposición 3.2.2** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$. Definimos*

$$\varphi_\alpha : E(K) \longrightarrow K^*/K^{*2}$$

*mediante*

$$\varphi_\alpha = \begin{cases} (x-\alpha)K^{*2} & \text{si } P = (x,y) \text{ con } P \neq \mathcal{O} \text{ y } x \neq \alpha, \\ (\alpha-\beta)(\alpha-\gamma)K^{*2} & \text{si } P = (\alpha, 0), \\ 1 \cdot K^{*2} & \text{si } P = \mathcal{O}. \end{cases}$$

*Entonces $\varphi_\alpha$ es un homomorfismo de grupos.*

**Corolario.** *$\varphi_\alpha$ induce un homomorfismo de grupos*

$$E(K)/2E(K) \longrightarrow K^*/K^{*2},$$

*que llamaremos también $\varphi_\alpha$.*

*Demostración Proposición* 3.2.2 : Si tenemos $P_1 \oplus P_2 = P_3$ con $P_i \in E(K)$ para $i = 1, 2, 3$, queremos comprobar que

$$\varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3)^{-1} \in K^{*2}.$$

Observamos que si $k \in K^*/K^{*2}$, entonces $k = k^{-1}$. Además, por la definición de $\varphi_\alpha$, para todo $P \in E(K)$ se tiene $\varphi_\alpha(P) = \varphi_\alpha(\ominus P)$. Por tanto, para ver que $\varphi_\alpha$ es un homomorfismo de grupos basta con ver que

$$P_1 \oplus P_2 \oplus P_3 = \mathcal{O} \Longrightarrow \varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) \in K^{*2}.$$

Si $P_i = \mathcal{O}$, por ejemplo $i = 1$, entonces $P_2 \oplus P_3 = \mathcal{O}$. Por tanto como $\varphi_\alpha(P_2) = \varphi_\alpha(\ominus P_3) = \varphi_\alpha(P_3)$ se tiene

$$\varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) = [\varphi_\alpha(P_2)]^2 \in K^{*2}.$$

Es decir, podemos asumir que $P_i$ es un elemento de la forma $(x_i, y_i)$ con $i = 1, 2, 3$.

Vamos a diferenciar dos casos:

1. $x_i \neq \alpha$, $i = 1, 2, 3$.

   Sea $y = mx + b$ la recta que une $P_1, P_2, P_3$. Cada $P_i = (x_i, y_i)$ satisface

   $$(x - \alpha)(x - \beta)(x - \gamma) = y^2 = (mx + b)^2.$$

   Entonces $(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = 0$ para $x = x_1, x_2, x_3$. Es decir,

   $$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = (x - x_1)(x - x_2)(x - x_3).$$

   Poniendo $x = \alpha$ obtenemos

   $$(x_1 - \alpha)(x_2 - \alpha)(x_3 - \alpha) = (m\alpha + b)^2;$$

   y por la definición de $\varphi_\alpha$, tenemos

   $$\varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) \in K^{*2}.$$

2. $x_1 = \alpha$.

   Entonces $(x_2, y_2), (x_3, y_3) \neq (\alpha, 0)$, ya que si no alguno de los tres puntos sería $\mathcal{O}$, posibilidad que hemos descartado anteriormente. Sea de nuevo $y = mx + b$ la recta que une $P_1, P_2, P_3$. Ahora, como $x_1 = \alpha$, obtenemos

   $$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = (x - \alpha)(x - x_2)(x - x_3). \tag{3.2}$$

   Entonces $(x - \alpha) \mid (mx + b)^2$, y por lo tanto $mx + b = m(x - \alpha)$. Sustituyendo en la ecuación (3.2) tenemos

   $$(x - \alpha)(x - \beta)(x - \gamma) - m^2(x - \alpha)^2 = (x - \alpha)(x - x_2)(x - x_3);$$

   y dividiendo por $x - \alpha$,

   $$(x - \beta)(x - \gamma) - m^2(x - \alpha) = (x - x_2)(x - x_3).$$

   Tomando $x = \alpha$ conseguimos

   $$(\alpha - \beta)(\alpha - \gamma) = (\alpha - x_2)(\alpha - x_3),$$

   que no es más que

   $$\varphi_\alpha(P_1) = \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3).$$

   Luego

   $$\varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) \in K^{*2}.$$

□

**Lema 3.2.3** *Sea $E$ una curva elíptica definida sobre $K$ con $car(K) \neq 2, 3$. Supongamos que $E$ está dada por*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) = x^3 + rx^2 + sx + t \quad \text{con } \alpha, \beta, \gamma \in K.$$

*Dado $P_2 = (x_2, y_2) \in E(K)$, $P_2 \neq \mathcal{O}$, existe $P_1 = (x_1, y_1) \in E(K)$ tal que $[2]P_1 = P_2$ si y sólo si*

$$\begin{cases} x_2 - \alpha = \alpha_1^2 \\ x_2 - \beta = \beta_1^2 \\ x_2 - \gamma = \gamma_1^2 \end{cases} \qquad \text{con } \alpha_1, \beta_1, \gamma_1 \in K.$$

*Demostración*:
$\boxed{\Rightarrow}$ Supongamos que existe $P_1 = (x_1, y_1)$ tal que $[2]P_1 = P_2$. Sea $y = mx + b$ la recta tangente a $E$ en $P_1$. La recta corta a $E$ en $P_1$ dos veces y en $P_2$. Por tanto las raíces de

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = 0$$

son $x_1$, como raíz doble, y $x_2$. Entonces tenemos

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = (x-x_2)(x-x_1)^2.$$

Pongamos $x = \alpha$:

$$-(mx+b)^2 = (\alpha - x_2)(\alpha - x_1)^2.$$

Es obvio que $\alpha - x_1 \neq 0$, ya que si $x_1 = \alpha$, entonces $P_1 = (\alpha, 0)$ y tendríamos $[2]P_1 = \mathcal{O} = P_2$, en contradicción con la hipótesis $P_2 \neq \mathcal{O}$. Por tanto,

$$x_2 - \alpha = \left(\frac{m\alpha + b}{\alpha - x_1}\right)^2 = \alpha_1^2.$$

Análogamente para $\beta$ y $\gamma$.

$\boxed{\Leftarrow}$ Para simplificar, vamos a hacer un cambio de variables, para así tener $x_2 = 0$ y con esto obtener $y_2^2 = -\alpha\beta\gamma = t$. Por tanto tenemos como hipótesis

$$\begin{cases} -\alpha = \alpha_1^2 \\ -\beta = \beta_1^2 \\ -\gamma = \gamma_1^2 \end{cases} \qquad \text{con } \alpha_1, \beta_1, \gamma_1 \in K.$$

Entonces podemos elegir

$$y_2 = \alpha_1\beta_1\gamma_1.$$

Busquemos ahora $P_1$. Sea $y = mx + b$ una recta que pasa por $P_2$ y es tangente a $E$ en un punto $(x_1, y_1)$, es decir,

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = x(x-x_1)^2.$$

Observamos que $y_2 = b$ ya que $y = mx + b$ pasa por $(0, y_2)$. Entonces,

$$\frac{1}{x}\left[x^3 + rx^2 + sx - m^2x^2 - 2my_2x\right] = (x-x_1)^2,$$

esto es, el polinomio

$$x^2 + rx + s - m^2x - 2my_2 \tag{3.3}$$

tiene raíces repetidas. Por tanto su discriminante es nulo,

$$(m^2 - r)^2 - 4(s - 2my_2) = 0. \tag{3.4}$$

Si encontramos una solución $m_0 \in K$ de la ecuación (3.4) obtendríamos que $x_1 = \frac{1}{2}(m_0^2 - r)$ es una raíz doble de (3.3), y que por tanto

$$[2](x_1, m_0x_1 + y_2) = (x_2, -y_2) = \ominus P_2.$$

Con esto,

$$[2](x_1, -m_0x_1 - y_2) = P_2.$$

Vamos a buscar una solución de (3.4). Introducimos una nueva variable $u$:

$$(m^2 - r + u)^2 = (m^2 - r)^2 + 2um^2 - 2ur + u^2$$

y utilizando (3.4),

$$(m^2-r+u)^2 = 4(s-2my_2)+2um^2-2ur+u^2 = 2um^2-8y_2m+u^2-2ur+4s. \tag{3.5}$$

El lado derecho de esta ecuación es el cuadrado de un polinomio en $m$. Para verlo, necesitamos encontrar una raíz doble de $2um^2 - 8y_2m + u^2 - 2ur + 4s$, y para ello el discriminante ha de ser cero:

$$64y_2^2 - 8u(u^2 - 2ru + 4s) = 0.$$

Utilizando que $y_2^2 = t$, tenemos

$$-u^3 + 2ru^2 - 4su + 8t = 0.$$

Las raíces de esta ecuación son $-2\alpha, -2\beta$ y $-2\gamma$, por serlo $\alpha, \beta$ y $\gamma$ de la ecuación $x^3 + rx^2 + sx + t = 0$. Y si ponemos $u = -2\alpha$ en (3.5),

$$(m^2 - r - 2\alpha)^2 = -4\alpha m^2 - 8y_2m + 4\alpha^2 + 4r\alpha + 4s.$$

Ahora podemos escribir $r$ y $s$ en términos de $\alpha, \beta, \gamma$, deduciendo

$$\begin{cases} r = -(\alpha + \beta + \gamma), \\ s = \alpha\beta + \alpha\gamma + \beta\gamma; \end{cases}$$

y utilizando

$$\begin{cases} -\alpha = \alpha_1^2, \\ -\beta = \beta_1^2, \\ -\gamma = \gamma_1^2, \end{cases}$$

junto con $y_2 = \alpha\beta\gamma$ obtenemos

$$(m^2 - \alpha + \beta + \gamma)^2 = 4(\alpha_1 m - \beta_1\gamma_1)^2.$$

Así que

$$\begin{aligned} m^2 - \alpha + \beta + \gamma &= \pm 2(\alpha_1 m - \beta_1\gamma_1) \\ m^2 \mp 2\alpha_1 m - \alpha &= -\beta - \gamma \mp 2\beta_1\gamma_1 \\ (m \mp \alpha_1)^2 &= \beta_1^2 \mp 2\beta_1\gamma_1 + \gamma_1^2 = (\beta_1 \mp \gamma_1)^2. \end{aligned}$$

En definitiva, obtenemos las siguientes soluciones de (3.4):

$$\begin{aligned} m &= \alpha_1 \pm (\beta_1 - \gamma_1) \\ m &= \alpha_1 \pm (\beta_1 + \gamma_1) \\ m &= -\alpha_1 \pm (\beta_1 - \gamma_1) \\ m &= -\alpha_1 \pm (\beta_1 + \gamma_1), \end{aligned}$$

todas ellas pertenecientes a $K$. Así queda demostrado el Lema.

□

Análogamente a la definición de $\varphi_\alpha$, podemos definir $\varphi_\beta$. Así obtenemos la siguiente proposición:

**Proposición 3.2.4** *El homomorfismo*

$$\varphi_\alpha \times \varphi_\beta : E(K)/2E(K) \longrightarrow K^*/K^{*2} \times K^*/K^{*2},$$

*es inyectivo.*

*Demostración*: Sea $P \neq \mathcal{O}$, de la forma $(x, y)$. Supongamos que $P \in \ker \varphi_\alpha \times \varphi_\beta$, de forma que

$$\varphi_\alpha(P), \varphi_\beta(P) \in K^{*2}.$$

Vamos a diferenciar varios casos:

1. $P \neq (\alpha, 0), (\beta, 0)$. La hipótesis es que $x - \alpha, x - \beta \in K^{*2}$. Además como $P \in E(K)$,
$$(x - \alpha)(x - \beta)(x - \gamma) = y^2 \in K^{*2},$$
luego $x - \gamma \in K^{*2}$ y por el lema 3.2.3 tedremos que $P \in 2E(K)$.

2. $P = (\alpha, 0)$. La hipótesis es ahora que
$$\left\{ \begin{array}{l} \varphi_\alpha(P) \in K^{*2} \\ \varphi_\beta(P) \in K^{*2} \end{array} \right. \quad \text{es decir} \quad \left\{ \begin{array}{l} (\alpha - \beta)(\alpha - \gamma) \in K^{*2} \\ (\beta - \alpha) \in K^{*2} \end{array} \right. ,$$
por tanto,
$$\left\{ \begin{array}{l} \alpha - \beta \in K^{*2} \\ \alpha - \gamma \in K^{*2} \end{array} \right. .$$
Además $\alpha - \alpha = 0 \in K^{*2}$. Aplicando de nuevo el lema 3.2.3 obtenemos que $P = (\alpha, 0) \in 2E(K)$.

3. $P = (\beta, 0)$. Totalmente análogo al caso 2.

□

Necesitamos ahora enunciar un Teorema que se enmarca en la Teoría Algebraica de Números. Se puede demostrar, aunque no lo haremos, utilizando técnicas básicas de dicha teoría (ver [KNA]). Una introducción a la Teoría Algebraica de Números se puede encontrar en [S-T] o [SAM].

**Teorema 3.2.5** *Sea $K$ un cuerpo de números y sea $\mathcal{O}_K$ el anillo de enteros de $K$. Entonces existe un anillo $R$ con $\mathcal{O}_K \subseteq R \subseteq K$ tal que:*

*(i) $R$ es un dominio de ideales principales y por lo tanto, un dominio de factorización única.*

*(ii) El grupo de unidades de $R$ está finitamente generado.*

Construido este anillo $R$, tenemos que por ser un dominio de factorización única, podemos escribir

$$K^*/K^{*2} = \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{p \text{ primo en } R} \mathbb{Z}/2\mathbb{Z}, \tag{3.6}$$

donde $\mathcal{U}(R)$ denota el conjunto de unidades de $R$ y $\mathcal{U}^2(R)$, el de los cuadrados de las unidades de $R$.

Veremos que la imagen de $\varphi_\alpha \times \varphi_\beta$ en $K^*/K^{*2} \times K^*/K^{*2}$ es cero en casi todas las coordenadas de la descomposición de $K^*/K^{*2} \times K^*/K^{*2}$ obtenida aplicando (3.6) a los dos factores.

Si $p$ es un primo en $R$ y $r$ es un elemento de $K$, escribiremos $p^a \parallel r$ si $r = p^a q$ y $q \in K$ es tal que $p$ no es un factor ni de su denominador ni de su numerador. Utilizaremos todo esto para ver que $E(K)/2E(K)$ es finito.

**Observación 3.2.6** Si $K$ es el cuerpo de fracciones de un dominio $R$ y $E$ es una curva elíptica dada por

$$y^2 = x^3 + Ax + B \quad A, B \in K,$$

podemos tomar $r$ el mínimo común denominador de $A$ y $B$, y hacer el cambio

$$\begin{cases} X = r^2 x, \\ Y = r^3 y. \end{cases}$$

Con esto, podemos suponer que $A, B \in R$. En particular, si $K = \mathbb{Q}$, la curva elíptica $E$ tiene una forma de Weierstrass de la forma

$$y^2 = x^3 + Ax + B \quad \text{con } A, B \in \mathbb{Z}.$$

Además, si $x^3 + Ax + B = (x - \alpha)(x - \beta)(x - \gamma) = f(x) \in \mathbb{Z}[x]$ y $K$ es el cuerpo de descomposición del polinomio $f(x)$, entonces por lo anterior, se deduce que $\alpha, \beta, \gamma \in \mathcal{O}_K$.

**Proposición 3.2.7** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$, por la observación anterior, podemos suponer que $E$ viene dada por la ecuación*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) = f(x) \qquad \text{con } \alpha, \beta, \gamma \in \mathcal{O}_K,$$

*donde $K$ es el cuerpo de descomposición de $f(x)$. Sea $\varphi_\alpha \times \varphi_\beta$ el homomorfismo anteriormente definido y $d$ el discriminante de $f(x)$. Entonces el homomorfismo inducido por $\varphi_\alpha \times \varphi_\beta$,*

$$E(K)/2E(K) \longrightarrow \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{\substack{p \text{ primo en } R \\ \text{tal que } p \mid d}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}),$$

*es inyectivo.*

*Demostración*: Sea $P = (x, y) \in E(K) \setminus \{\mathcal{O}\}$. Queremos comprobar que las coordenadas de $P$ en la descomposición (3.6) correspondientes a primos $p$ que no dividan a $d$ son cero.

Fijamos un primo $p \in R$ y definimos los enteros $a, b, c$ como

$$p^a \parallel (x-\alpha), \qquad p^b \parallel (x-\beta), \qquad p^c \parallel (x-\gamma).$$

Como $(x-\alpha)(x-\beta)(x-\gamma) = y^2$ se debe cumplir que

$$a + b + c \equiv 0 \bmod 2. \tag{3.7}$$

Cuando $x \neq \alpha, \beta, \gamma$ vamos a diferenciar dos casos:

1. Al menos uno de $a, b, c$ es $< 0$. Digamos $a < 0$. Como $\alpha \in \mathcal{O}_K$ y $\mathcal{O}_K \subseteq R$, entonces $\alpha \in R$, y por tanto,

   $$p^{|a|} \parallel (\text{denominador de } x).$$

   Con esto tenemos que $p^a \parallel (x-\alpha), (x-\beta), (x-\gamma)$. Es decir, $a = b = c$ y de (3.7) deducimos que

   $$a \equiv b \equiv c \equiv 0 \, mod \, 2.$$

   Luego la imagen de $P = (x, y)$ en la $p$-ésima coordenada de la descomposición (3.6) es cero.

2. Al menos uno de $a, b, c$ es $> 0$. Digamos $a > 0$. Si $p \not| d$, entonces $p \not| (\alpha - \beta)$. Como

   $$x - \beta = (x - \alpha) + (\alpha - \beta),$$

   y $a > 0$, se tiene $b = 0$. Análogamente, con $(\alpha - \gamma)$ obtenemos $c = 0$. Y usando de nuevo (3.7) llegamos a

   $$a \equiv b \equiv c \equiv 0 \, mod \, 2.$$

   Por tanto la imagen de $P = (x, y)$ en la $p$-ésima coordenada de la descomposición (3.6) es de nuevo cero.

Nos queda por ver el caso en que $P \in \{(\alpha,0),(\beta,0),(\gamma,0)\}$. Para éstos, $\varphi_\alpha(P)$ y $\varphi_\beta(P)$ son productos de $(\alpha-\beta),(\alpha-\gamma)$ y $(\beta-\gamma)$. Si $p\not| d$, entonces $p\not|(\alpha-\beta), p\not|(\alpha-\gamma)$ y $p\not|(\beta-\gamma)$, por tanto $a=b=c=0$.

Se concluye que la imagen de cualquier $P=(x,y)$ en todas las coordenadas tales que $p\not| d$ de la descomposición (3.6) son cero.

□

Ahora, como el grupo de unidades de $R$, $\mathcal{U}(R)$, es finitamente generado,

$$\{\mathcal{U}(R)/\mathcal{U}^2(R)\}$$

es finito. Por lo tanto el grupo

$$\{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{\substack{p \text{ primo en } R \\ \text{tal que } p \,|\, d}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$$

es finito, y utilizando esto último junto con la proposición 3.2.7 obtenemos que $E(K)/2E(K)$ es finito.

Para demostrar el Teorema débil de Mordell, sólo nos queda aplicar el corolario de la proposición 3.2.1 al hecho de que $E(K)/2E(K)$ es finito, para así obtener que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.

**Observación 3.2.8** En el caso particular de que $\alpha,\beta,\gamma \in \mathbb{Z}$ podíamos haber demostrado la proposición 3.2.7 sobre $\mathbb{Q}$, en lugar de $K$, sin necesidad de utilizar el anillo auxiliar $R$, haciendo las mismas demostraciones para $\mathbb{Z}$ y teniendo en cuenta que $\mathcal{U}(\mathbb{Z})=\{\pm 1\}$, y por tanto $\mathcal{U}(\mathbb{Z})/\mathcal{U}^2(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

$$\begin{array}{ccc}
E(\mathbb{Q})/2E(\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \oplus \displaystyle\bigoplus_{\substack{p \text{ primo en } \mathbb{Z} \\ \text{tal que } p \,|\, d}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \\
\downarrow & & \downarrow \\
\mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} & = & (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \oplus \displaystyle\bigoplus_{p \text{ primo en } \mathbb{Z}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})
\end{array}$$

## 3.3 El Teorema de Mordell.

En esta sección demostraremos el teorema de Mordell-Weil en el caso que más nos interesa, esto es, para curvas elípticas definidas sobre $\mathbb{Q}$. En este caso el teorema es llamado teorema de Mordell y su demostración fue publicada en 1922 en [MOR1].

**Teorema de Mordell.** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$. Entonces $E(\mathbb{Q})$ es un grupo abeliano finitamente generado.*

Vamos a dar una función altura explícita para poder aplicar el teorema del descenso.

**Definición.** *Sea $x = \dfrac{p}{q} \in \mathbb{Q}$ con $(p,q) = 1$. Se define la* **altura de** *$x$ como*

$$H(x) = \max\{|p|, |q|\}.$$

**Definición.** *Se llama* **altura en** *$E(\mathbb{Q})$ a la función*

$$h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

*definida por*

$$h_x(P) = \begin{cases} log\, H(x(P)) & si\ P \neq \mathcal{O} \\ 0 & si\ P = \mathcal{O}. \end{cases}$$

Se tiene que $h_x(P)$ es no negativa para todo elemento $P$ de $E(\mathbb{Q})$.

**Proposición 3.3.1** *La función altura en $E(\mathbb{Q})$, $h_x$, satisface:*

*(i) Sea $Q \in E(\mathbb{Q})$. Existe una constante $C_1$, dependiendo de $Q, A$ y $B$, tal que para todo $P \in E(\mathbb{Q})$*

$$h_x(P \oplus Q) \leq 2h_x(P) + C_1.$$

*(ii) Existe una constante $C_2$, dependiendo de $A$ y $B$, tal que para todo $P \in E(\mathbb{Q})$,*

$$h_x([2]P) \geq 4h_x(P) - C_2.$$

*(iii) Para cualquier constante $C_3$, el conjunto*

$$\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$$

*es finito.*

Antes de la demostración de la proposición haremos algunas observaciones.

**Observación 3.3.2** Cualquier número racional $q \neq 0$ puede ser puesto en la forma

$$q = p^{\nu}\frac{m}{n},$$

donde $m, n \in \mathbb{Z}$ son tales que $p \nmid m, n$ y $(m, n) = 1$. Definimos el orden $p$-ádico de un número racional como el entero $\nu$, y escribimos

$$ord_p(q) = ord_p\left(p^{\nu}\frac{m}{n}\right) = \nu.$$

Sea $E$ la curva elíptica dada por

$$E : y^2 = x^3 + Ax + B \qquad \text{con } A, B \in \mathbb{Z},$$

y supongamos que $p$ divide al denominador de $x$ y no al numerador, esto es,

$$(x, y) = \left(\frac{m}{np^{\mu}}, \frac{u}{wp^{\sigma}}\right),$$

donde $\mu > 0$ y $p \nmid m, n, u, w$. Como $(x, y) \in E(\mathbb{Q})$ se tiene que

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + Amn^2p^{2\mu} + Bn^3p^{3\mu}}{n^3p^{3\mu}}.$$

Tenemos que $p \nmid u^2$ y $p \nmid w^2$, por lo que

$$ord_p\left(\frac{u^2}{w^2p^{2\sigma}}\right) = -2\sigma.$$

Como $\mu > 0$ y $p \nmid m$, se obtiene

$$p \nmid (m^3 + Amn^2p^{2\mu} + Bn^3p^{3\mu}),$$

y por tanto,

$$ord_p\left(\frac{m^3 + Amn^2p^{2\mu} + Bn^3p^{3\mu}}{n^3p^{3\mu}}\right) = -3\mu.$$

Luego

$$2\sigma = 3\mu. \tag{3.8}$$

En particular $\sigma > 0$ y por ello $p$ divide al denominador de $y$. Además, la relación (3.8) nos dice que

$$2 \,|\, \mu \quad \text{y} \quad 3 \,|\, \sigma.$$

Así que concluimos que

$$\mu = 2\nu \quad \text{y} \quad \sigma = 3\nu,$$

con $\nu \in \mathbb{Z}$ y $\nu > 0$.

Análogamente, si $p$ divide al denominador de $y$ sin dividir a su numerador, llegamos al mismo resultado. Por lo tanto, si hacemos esto para todos los primos, podemos concluir que

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right),$$

con $(a, b, d) = 1$ y $a, b, d \in \mathbb{Z}$.

**Observación 3.3.3** Sea $d = 4A^3 + 27B^2$ y sean

$$F(x,z) = x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4,$$
$$G(x,z) = 4x^3z + 4Axz^3 + 4Bz^4.$$

Entonces existen $f_1, f_2, g_1, g_2 \in \mathbb{Q}[x,z]$ tales que se tienen las siguientes igualdades:

$$f_1(x,z)F(x,z) - g_1(x,z)G(x,z) = 4dz^7,$$
$$f_2(x,z)F(x,z) - g_2(x,z)G(x,z) = 4dx^7.$$

Para demostrar este hecho, basta con dar $f_1, f_2, g_1, g_2$ y ver que las igualdades anteriores se cumplen. Estos polinomios son:

$$f_1 = -4(3x^2z + 4Az^3),$$
$$g_1 = 27Bz^3 + 5Axz^2 - 3x^3,$$
$$f_2 = -4(dx^3 - A^2Bx^2z + (3A^2 + 22AB^2)xz^2 + 3(A^3B + 8B^3)z^3),$$
$$g_2 = A^2Bx^3 + (5A^4 + 32AB^2)x^2z + (26A^3B + 192B^3)xz^2 - 3(A^5 + 8A^2B^2)z^3.$$

*Demostración de la proposición 3.3.1*:

(i) Vamos a diferenciar varios casos:

- Si $Q = \mathcal{O}$ es obvio que $h_x(P \oplus \mathcal{O}) = h_x(P) < 2h_x(P) + 1$. Tomando $C_1 = 1$ obtendríamos el resultado deseado.
- Si $P = \mathcal{O}$, $Q$, $\ominus Q$.
  - Si $P = \mathcal{O}$, igual que en el caso anterior.
  - Si $P = \ominus Q$, $h_x(\ominus Q \oplus Q) = h_x(\mathcal{O}) = 0 < 2h_x(\ominus Q) + 1$, y tomamos $C_1 = 1$.
  - Si $P = Q$,
    $$h_x(Q \oplus Q) = h_x([2]Q) < 2h_x(Q) + C_1,$$
    con $C_1 > \max\{h_x(Q), h_x([2]Q)\}$.
- Ahora tomamos $Q \neq \mathcal{O}$ y $P \neq \mathcal{O}, Q, \ominus Q$.
  Por la observación 3.3.2 podemos escribir $P$ y $Q$ en la forma
  $$P = (x,y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \quad \text{y} \quad Q = (x',y') = \left(\frac{a'}{d'^2}, \frac{b'}{d'^3}\right),$$
  con $(a,b,d) = 1$ y $(a',b',d') = 1$ y $a,b,d,a',b',d' \in \mathbb{Z}$. Usando la fórmula de la suma $\oplus$ en $E(\mathbb{Q})$, obtenemos
  $$\begin{aligned} x(P \oplus Q) &= \left(\frac{y-y'}{x-x'}\right)^2 - (x - x') = \frac{(xx' + A)(x + x') + 2B - 2yy'}{(x-x')^2} \\ &= \frac{(aa' + Ad^2d'^2)(ad'^2 + a'd^2) + 2Bd^4d'^4 - 2bdb'd'}{(ad'^2 - a'd^2)^2}. \end{aligned}$$

Al calcular la altura de un número racional, las cancelaciones entre el numerador y el denominador sólo contribuyen a que la altura decrezca. Usando la desigualdad

$$\left|\sum_{i=1}^{n} A_i B_i\right| \leq n \cdot \max_{1\leq i\leq n}\{|A_i|\} \max_{1\leq i\leq n}\{|B_i|\}, \tag{3.9}$$

y por la definición de altura, obtenemos que

$$H(x(P\oplus Q)) \leq C_1' \max\{|a^2|, |d^4|, |ad^2|, |bd|\} \leq C_1' \max\{|a|^2, |d|^4, |bd|\}$$

donde $C_1'$ depende de $A, B, a', b', c'$. Como $P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \in E(\mathbb{Q})$, entonces

$$b^2 = a^3 + Aad^4 + Bd^6,$$

por lo que

$$|b| \leq C_1'' \max\{|a|^{3/2}, |d|^3\}.$$

Entonces

$$|bd| \leq C_1'' \max\{|a|^{3/2}|d|, |d|^4\}.$$

Ahora vamos a ver que

$$\max\{|a|^{3/2}|d|, |d|^4\} \leq \max\{|a|^2, |d|^4\}.$$

Si $|a|^{3/2} \leq |d|^3 \Longrightarrow \max\{|a|^{3/2}|d|, |d|^4\} \leq |d|^4$.
Si $|a|^{3/2} \geq |d|^3 \Longrightarrow \max\{|a|^{3/2}|d|, |d|^4\} \leq |a|^{3/2} \leq |a|^2$.
Por lo tanto,

$$|bd| \leq C_1'' \max\{|a|^2, |d|^4\}.$$

Así obtenemos

$$H(x(P\oplus Q)) \leq C_1' C_1'' \max\{|a|^2, |d|^4\} = C_1' C_1'' H^2(x(P)),$$

y tomando logaritmos,

$$log\, H(x(P\oplus Q)) \leq log(C_1' C_1'') + 2log\, H(x(P));$$

es decir,

$$h_x(P\oplus Q) \leq 2h_x(P) + C_1,$$

donde $C_1 = log(C_1' C_1'')$ sólo depende de $A, B, a', b', d'$. Con lo que queda demostrado el apartado (i).

(ii) También vamos a distinguir varios casos.

- Si $P$ cumple $[2]P = \mathcal{O}$, tomando $C_2 > \max\{4h_x(P') : [2]P' = \mathcal{O}\}$ ya está.

– Ahora suponemos $[2]P \neq \mathcal{O}$. Sea $P = (x, y)$; entonces la fórmula de la suma $\oplus$ nos dice

$$x([2]P) = \left(\frac{f'(x)}{2y}\right)^2 - 2x = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

Los polinomios homogeneizados del numerador y del denominador de $x([2]P)$ son

$$\begin{aligned} F(x, z) &= x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4, \\ G(x, z) &= 4x^3z + 4Axz^3 + 4Bz^4, \end{aligned}$$

así que, si $x = \dfrac{a}{b}$ con $(a, b) = 1$,

$$x([2]P) = \frac{F(a, b)}{G(a, b)}.$$

A diferencia del apartado (i), estamos buscando una cota inferior para la altura de $x([2]P)$, por lo que hay que controlar las cancelaciones entre el numerador y el denominador. Tenemos

$$\begin{aligned} F(x, 1) &= f'(x) - 8xf(x), \\ G(x, 1) &= 4f(x), \end{aligned}$$

que son primos entre sí, ya que $f(x)$ y $f'(x)$ son primos entre sí por ser $E$ una curva lisa. Sea $\delta = mcd\{F(a, b), G(a, b)\}$; entonces por la observación 3.3.3 se cumplirá que

$$\begin{cases} \delta \mid 4db^7, \\ \delta \mid 4da^7; \end{cases}$$

y como $(a, b) = 1$ tenemos que $\delta$ divide a $4d$. Por tanto,

$$|\delta| \leq |4d|.$$

Con esta última desigualdad,

$$H(x([2]P)) \geq \frac{\max\{|F(a, b)|, |G(a, b)|\}}{|4d|}. \tag{3.10}$$

Por otra parte, utilizando de nuevo la observación 3.3.3 y la desigualdad (3.9),

$$\begin{aligned} |4db^7| &\leq 2\max\{|f_1(a, b)|, |g_1(a, b)|\} \max\{|F(a, b)|, |G(a, b)|\}, \\ |4da^7| &\leq 2\max\{|f_2(a, b)|, |g_2(a, b)|\} \max\{|F(a, b)|, |G(a, b)|\}. \end{aligned}$$

Ahora viendo cómo son $f_1, g_1, f_2, g_2$ tenemos

$$\begin{aligned} &\max\{|f_1(a, b)|, |g_1(a, b)|, |f_2(a, b)|, |g_2(a, b)|\} \leq \\ &\quad \leq C(A, B)\ \max\{|a^2b|, |b^3|, |a^3|, |ab^2|\} = C(A, B)\ \max\{|b^3|, |a^3|\}, \end{aligned}$$

con $C(A,B)$ una constante dependiendo de $A$ y $B$. Reuniendo las tres últimas desigualdades obtenemos:

$$\max\{|4da^7|, |4db^7|\} \leq 2C(A,B)\max\{|a^3|, |b^3|\}\max\{|F(a,b)|, |G(a,b)|\}$$
$$\max\{|a^4|, |b^4|\} \leq 2C(A,B)\frac{\max\{|F(a,b)|, |G(a,b)|\}}{|4d|}.$$

Ahora, utilizando (3.10),

$$\max\{|a^4|, |b^4|\} \leq 2C(A,B)\, H(x([2]P)),$$

y usando la definición de altura,

$$\frac{1}{2C(A,B)}H^4(x(P)) \leq H(x([2]P)).$$

Si tomamos logaritmos,

$$4h_x(P) - C_2 \leq h_x([2]P)$$

donde $C_2 = log(2C(A,B))$ es una constante que sólo depende de $A$ y $B$.

Por tanto hemos demostrado (ii).

(iii) Para cualquier constante $C \geq 0$, se tiene que el conjunto

$$\{q \in \mathbb{Q} : H(q) \leq C\}$$

es claramente finito, ya que si $q = \frac{a}{b} \in \mathbb{Q}$ con $(a,b) = 1$, entonces $H(q) = \max\{|a|, |b|\}$. Por tanto si $H(q) \leq C$, entonces $|a| \leq C$ y $|b| \leq C$ y por ser $a$ y $b$ números enteros sólo existen una cantidad de ellos cumpliendo esa acotación. De hecho,

$$\#\{q \in \mathbb{Q} : H(q) \leq C\} \leq (2C+1)^2.$$

En nuestra curva elíptica, para cada $x$ hay como mucho dos valores para $y$ para los que el punto $(x,y)$ pertenece a la curva. Por tanto,

$$\#\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\} < \infty.$$

□

**Demostración del Teorema de Mordell**: El teorema débil de Mordell nos dice que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito. La proposición 3.3.1 nos asegura que la función $h_x : E(\mathbb{Q}) \to \mathbb{R}$ satisface las tres propiedades de las hipótesis de altura del Teorema del Descenso, por lo tanto el Teorema del Descenso nos asegura que $E(\mathbb{Q})$ está finitamente generado.

□

## 3.4 Generalizaciones del Teorema de Mordell.

En esta sección enunciaremos varias generalizaciones del Teorema de Mordell. La primera consistirá en considerar curvas elípticas definidas sobre cuerpos de números.

**Teorema de Mordell-Weil.** *Sea $E$ una curva elíptica definida sobre un cuerpo de números $K$. Entonces $E(K)$ es un grupo abeliano finitamente generado.*

La demostración de este resultado se basa, al igual que la del Teorema de Mordell, en la aplicación del Teorema del Descenso al grupo abeliano que forman los puntos racionales de $E$. Pero a diferencia del caso en que $K = \mathbb{Q}$, no podemos definir una función altura de forma tan explícita, por lo que se han de utilizar otras técnicas; y estas son las desarrolladas por la teoría general de funciones altura (ver [SIL], Capítulo VIII, Secciones 5 y 6). Para utilizar el Teorema del Descenso necesitamos que exista un entero $m \geq 2$ tal que $E(K)/mE(K)$ sea finito. Este resultado nos lo da el siguiente teorema, que no es más que una generalización del Teorema Débil de Mordell al caso de cuerpos de números (para la demostración, ver [SIL], Capítulo VIII, Teorema 1.1).

**Teorema Débil de Mordell-Weil.** *Sea $E$ una curva elíptica definida sobre un cuerpo de números $K$. Entonces para cualquier entero $m \geq 2$, $E(K)/mE(K)$ es un grupo finito.*

El siguiente paso es tomar variedades abelianas. Una **variedad abeliana** es una variedad proyectiva lisa $A$ definida sobre $\overline{K}$ que tiene un punto distinguido $\mathcal{O} \in A$ y una estructura de grupo abeliano para la que $\mathcal{O}$ es el elemento neutro de la operación suma en $A$ y las operaciones suma y resta en $A$ son morfismos. Además se dice que está **definida sobre** $K$ si $A$ está definida sobre $K$ como variedad proyectiva, y $\mathcal{O} \in A(K)$. Así una curva elíptica no es más que una variedad abeliana de dimensión 1. El resultado es el siguiente:

**Teorema de Weil.** *Sea $K$ un cuerpo cuerpo de números y sea $A$ una variedad abeliana definida sobre $K$. Entonces $A(K)$ está finitamente generado.*

Tanto este último teorema como el que hemos llamado Teorema de Mordell-Weil, fueron demostrados por A. Weil en 1928 ([WE1]). El mismo Weil, en 1930 ([WE2]), aplicó la demostración de este teorema al caso de curvas elípticas definidas sobre $\mathbb{Q}$, para así dar una prueba más sencilla que la que dió Mordell.

Por último, A. Neron ([NER1]) generalizó el Teorema de Weil al caso en que el cuerpo $K$ es un cuerpo finitamente generado sobre un cuerpo primo.

**Teorema de Mordell-Weil-Nerón.** *Sea $K$ un cuerpo finitamente generado sobre un cuerpo primo y sea $A$ una variedad abeliana definida sobre $K$. Entonces $A(K)$ está finitamente generado.*

# Capítulo 4

# Puntos de torsión.

Vimos en el capítulo anterior que si $E$ es una curva elíptica definida sobre $\mathbb{Q}$, entonces

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r,$$

donde $E(\mathbb{Q})_{tors}$ es un grupo finito denominado subgrupo de torsión de $E(\mathbb{Q})$ y $r$ es un entero no negativo llamado rango de $E$. En este capítulo estudiaremos el subgrupo de torsión de $E(\mathbb{Q})$.

En la sección §3.1 veremos el *Teorema de Nagell-Lutz*, que nos permitirá calcular explícitamente $E(\mathbb{Q})_{tors}$ para una curva elíptica $E/\mathbb{Q}$ dada. Para demostrar este teorema introduciremos la reducción módulo un primo $p$ y la filtración $p$-ádica.

En la sección §3.2 veremos ejemplos de la aplicación del *Teorema de Nagell-Lutz*. También enunciaremos el *Teorema de Mazur*, que nos caracterizará por completo los subgrupos de torsión de las curvas elípticas definidas sobre $\mathbb{Q}$. Al final de esta sección veremos dos teoremas que nos permitirán clasificar los subgrupos de torsión de determinadas familias de curvas elípticas definidas sobre $\mathbb{Q}$. Estos últimos resultados son consecuencia del teorema de Dirichlet de los primos en una progresión aritmética.

Enunciaremos diferentes resultados sobre el subgrupo de torsión $E(K)_{tors}$ de una curva elíptica definida sobre un cuerpo de números $K$. Aquí trataremos sobre la *Conjetura de acotación uniforme fuerte*, que es el análogo al teorema de Mazur reemplazando $\mathbb{Q}$ por un cuerpo de números $K$. Resaltaremos los avances más importantes hechos por Mazur, Kamienny, Merel, Parent, Oesterlé, ....

## 4.1 Teorema de Nagell-Lutz.

Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$ dada por una forma normal de Weierstrass

$$y^2 = x^3 + Ax + B \quad A, B \in \mathbb{Z},$$

y sea $\Delta \in \mathbb{Z}$ el discriminante de $E$. Por el Teorema de Mordell, $E(\mathbb{Q})$ es un grupo finitamente generado. Nuestro objetivo en este capítulo es estudiar el subgrupo de

torsión $E(\mathbb{Q})_{tors}$. La principal herramienta en el análisis será la reducción módulo un primo $p$ y el resultado fundamental será el Teorema de Nagell-Lutz, que nos permite determinar $E(\mathbb{Q})_{tors}$ explícitamente para cualquier curva elíptica $E/\mathbb{Q}$ dada.

**Teorema de Nagell-Lutz.** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$ con ecuación de Weierstrass*

$$y^2 = x^3 + Ax + B \quad A, B \in \mathbb{Z}.$$

*Sea $P = (x(P), y(P), 1) \in E(\mathbb{Q})_{tors} \setminus \{\mathcal{O}\}$. Entonces:*

*(i)* $x(P), y(P) \in \mathbb{Z}$.

*(ii)* $y(P) = 0$ *(entonces* $[2]P = \mathcal{O}$*) o bien* $y(P)^2 \mid 4A^3 + 27B^2$.

Este teorema fue demostrado en la década comprendida entre 1930 y 1940, independientemente por Nagell ([NAG2]) y Lutz ([LUT]).

**Observación 4.1.1** Hay que tener en cuenta que el teorema de Nagell-Lutz no nos da condiciones suficientes para encontrar los puntos de torsión, sólo nos da condiciones necesarias. Es fácil encontrar curvas elípticas definidas sobre $\mathbb{Q}$ que tengan puntos con coordenadas enteras tales que $y(P)^2$ divida a $d = 4A^3 + 27B^2$ pero que, sin embargo, no sean puntos de orden finito.

### 4.1.1 Reducción módulo $p$.

Sea $p$ un primo y $r \in \mathbb{Q}$, $r \neq 0$; entonces podemos escribir

$$r = p^n \frac{u}{v} \quad \text{con } u, v \in \mathbb{Z} \text{ con } p \not| u, v.$$

Definimos la **norma $p$-ádica**, denotada por $|\cdot|_p$ como

$$|r|_p = p^{-n} \quad \text{con } r = p^n \frac{u}{v} \text{ como antes.}$$

Y por convención tomaremos $|0|_p = 0$.

**Propiedades de $|\cdot|_p$:**

(i) $|r + s|_p \leq max\{|r|_p, |s|_p\}$ , la igualdad se alcanza si $|r|_p \neq |s|_p$.

(ii) $|rs|_p = |r|_p \cdot |s|_p$.

*Demostración:* La propiedad (ii) es clara. Para ver (i) escribimos

$$r = p^n \frac{u}{v} \quad \text{y} \quad s = p^m \frac{u'}{v'} \quad \text{con } p \not| u, v, u', v',$$

y suponemos que $n \leq m$. Por lo tanto,

$$r + s = p^n \left( \frac{u}{v} + p^{m-n} \frac{u'}{v'} \right) = p^n \frac{uv' + p^{m-n} u'v}{vv'},$$

y tenemos que $(vv', p) = 1$ y $(uv', p) = 1$, con lo que obtenemos (i).

La propiedad (i) se llama **desigualdad ultramétrica**, y en particular implica la desigualdad triangular

$$|r + s|_p \leq |r|_p + |s|_p. \tag{4.1}$$

Si definimos

$$d(x, y) = |x - y|_p,$$

entonces la desigualdad (4.1) implica la desigualdad triangular para $d$. Así $d$ es una métrica en $\mathbb{Q}$.

**Observación 4.1.2** Al igual que los números reales se construyen completando los racionales con respecto a la norma euclídea usual, los racionales pueden ser completados con respecto a la norma $p$-ádica $|\cdot|_p$ dando el cuerpo de los **números $p$-ádicos**, denotado por $\mathbb{Q}_p$.

Diremos que $\alpha \in \mathbb{Q}_p$ es un **entero $p$-ádico** si

$$|\alpha|_p \leq 1.$$

Por las propiedades (i) y (ii), los enteros $p$-ádicos forman un subanillo de $\mathbb{Q}_p$, conteniendo a $\mathbb{Z}$, que se denota por $\mathbb{Z}_p$.

Para evitar trabajar con compleciones, nos bastará trabajar con el anillo

$$\mathbb{Z}_{(p)} := \mathbb{Z}_p \cap \mathbb{Q} = \left\{ \frac{m}{n} \in \mathbb{Q} : (p, n) = 1 \right\}.$$

Si $\alpha \in \mathbb{Z}_{(p)}$, entonces

$$\alpha = p^n \frac{u}{v} \quad p \nmid u, v \text{ con } n \geq 0.$$

Entonces definimos la **reducción módulo $p$** como

$$\begin{array}{rcl} r_p : \mathbb{Z}_{(p)} & \longrightarrow & \mathbb{F}_p \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \\ \alpha & \longmapsto & r_p(\alpha) = \begin{cases} \dfrac{u}{v} & \text{si } n = 0 \\ \\ 0 & \text{si } n > 0. \end{cases} \end{array}$$

Es evidente que esta aplicación es un homomorfismo de anillos.

Haciendo abuso de notación, definimos

$$\begin{gathered} r_p : \mathbb{P}^2(\mathbb{Q}) \longrightarrow \mathbb{P}^2(\mathbb{F}_p) \\ r_p([x, y, z]) = [r_p(x), r_p(y), r_p(z)] \end{gathered} \tag{4.2}$$

con $x, y, z \in \mathbb{Z}_{(p)}$ y al menos uno de ellos tiene $|\cdot|_p = 1$. Diremos que el punto $[x, y, z]$ es un **representante de $p$ reducción**. Se observa que para cualquier punto

$[x, y, z] \in \mathbb{P}^2(\mathbb{Q})$ podemos multiplicarlo por un cierto $p^n$ para obtener un representante de $p$-reducción. Un representante de $p$-reducción es único salvo multiplicación por un elemento con $|\cdot|_p = 1$. Así que $r_p$ está bien definida como aplicación de $\mathbb{P}^2(\mathbb{Q})$ en $\mathbb{P}^2(\mathbb{F}_p)$.

Usando $r_p : \mathbb{P}^2(\mathbb{Q}) \longrightarrow \mathbb{P}^2(\mathbb{F}_p)$, podemos reducir una curva proyectiva plana definida sobre $\mathbb{Q}$ a otra módulo $p$.

Sea $C$ una curva proyectiva plana definida por un polinomio homogéneo de grado $m$, $G(x, y, z) \in \mathbb{Q}[x, y, z]$ de grado $m$. Multiplicando los coeficientes por una cierta constante distinta de 0, podemos asumir que todos los coeficientes de $G$ tienen $|\cdot|_p \leq 1$ y que al menos uno de ellos tiene $|\cdot|_p = 1$. Por lo tanto podemos asumir que $C$ está definida sobre $\mathbb{Z}_{(p)}$. Entonces podemos reducir los coeficientes de $G$ módulo $p$, obteniendo un polinomio $G_p(x, y, z) \in \mathbb{F}_p[x, y, z]$ distinto de cero. Aunque $G_p$ no esta unívocamente determinado, está definido de forma única salvo multiplicación por un escalar distinto de 0. Por lo tanto la curva

$$C_p = \{[x, y, z] \in \mathbb{P}^2(\mathbb{F}_p) : G_p(x, y, z) = 0\}$$

está bien definida.

**Proposición 4.1.3** *Sea $C/\mathbb{Q}$ una curva proyectiva plana. Bajo el homomorfismo de reducción $r_p : \mathbb{P}^2(\mathbb{Q}) \longrightarrow \mathbb{P}^2(\mathbb{F}_p)$ dado en* (4.2)*, la imagen de $C(\mathbb{Q})$ está contenida en $C_p(\mathbb{F}_p)$. Es decir,*

$$r_p(C(\mathbb{Q})) \subset C_p(\mathbb{F}_p).$$

*Demostración*: Normalizamos los coeficientes de $G$ como antes, cogemos el punto $(x_0, y_0, z_0)$, un representante de $p$ reducción de un punto en $\mathbb{P}^2(\mathbb{Q})$. Entonces,

$$[x_0, y_0, z_0] \in C(\mathbb{Q}) \Longleftrightarrow G(x_0, y_0, z_0) = 0,$$

y por ser $r_p$ homomorfismo, $r_p(G(x_0, y_0, z_0)) = 0$, es decir,

$$G_p(r_p(x_0), r_p(y_0), r_p(z_0)) = G_p(r_p(x_0, y_0, z_0)) = 0 \Longrightarrow r_p(x_0, y_0, z_0) \in C_p(\mathbb{F}_p).$$

□

**Proposición 4.1.4** *Sea $C/\mathbb{Q}$ una curva proyectiva plana de grado $m$ definida por un polinomio $G$, $L/\mathbb{Q}$ una recta y $P_0 = [x_0, y_0, z_0]$ un punto de $L$. Si $[x', y', z']$ es cualquier punto de $L$ tal que $[x', y', z'] \neq [x_0, y_0, z_0]$, entonces $I_P(C, L)$ es igual al orden en $t = 0$ de $\varphi(t) = G(x_0 + tx', y_0 + ty', z_0 + tz')$. Es decir,*

$$I_P(C, L) = ord_{t=0}(\varphi(t)).$$

*Demostración*: Ver [KNA], Proposición 2.9.

**Proposición 4.1.5** *Sea $C/\mathbb{Q}$ una curva proyectiva plana de grado $m$ definida por un polinomio $G$, $L/\mathbb{Q}$ una recta y $P_0 = [x_0, y_0, z_0]$ un punto de $L$. Si $C_p$ y $L_p$ son las curvas reducidas módulo $p$ de $C$ y $L$, respectivamente, entonces*

$$I_{P_0}(C, L) \leq I_{r_p(P_0)}(C_p, L_p).$$

*Demostración*: Sin pérdida de generalidad podemos suponer que $P_0$ es un representante de $p$ reducción y que los coeficientes de $G$ y $L$ están normalizados. Elegimos un representante de $p$ reducción $[x', y', z']$ de un punto $P'$ de $L$ con la propiedad

$$[x', y', z'] \neq [x_0, y_0, z_0],$$

y la función

$$\varphi(t) = G(P_0 + tP) = G(x_0 + tx', y_0 + ty', z_0 + tz') = t^r F'_r + \ldots + t^m F'_m,$$

con $F'_r \neq 0$. Por la proposición 4.1.4 se tiene que

$$I_P(C, L) = ord_{t=0}(\varphi(t)) = r.$$

Tomando $\varphi(t)$ módulo $p$ y aplicando de nuevo la proposición 4.1.4 vemos que

$$I_P(C_p, L_p) \geq r.$$

□

Ahora vamos a aplicar las proposiciones 4.1.3 y 4.1.5 a curvas elípticas definidas sobre $\mathbb{Q}$.

Consideramos una curva elíptica $E/\mathbb{Q}$; podemos suponer que $E$ está en la forma normal de Weierstrass siguiente:

$$zy^2 = x^3 + Axz^2 + Bz^3 \quad \text{con } A, B \in \mathbb{Z}.$$

Los coeficientes de $E$ están en $\mathbb{Z}$, por lo tanto son enteros $p$-ádicos. Además $zy^2$ y $x^3$ tienen coeficiente 1, luego $E_p$ está dada por la ecuación

$$zy^2 = x^3 + \bar{A}xz^2 + \bar{B}z^3 \quad \text{con } \bar{A}, \bar{B} \in \mathbb{F}_p \text{ con } \bar{A} = A \bmod p, \bar{B} = B \bmod p.$$

Así definida $E_p$, el discriminante de $E_p$ es

$$\Delta_p = \Delta \bmod p.$$

Entonces se tiene

$$E_p \text{ es lisa} \iff p \not| \Delta.$$

La aplicación reducción $r_p$ restringida a $E(\mathbb{Q})$ nos da, por la proposición 4.1.3, una aplicación

$$r_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p). \tag{4.3}$$

**Proposición 4.1.6** *Si $E_p$ es lisa, entonces $r_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p)$ es un homomorfismo de grupos.*

*Demostración*: Tenemos $r_p([0,1,0]) = [0,1,0]$, es decir $r_p$ manda $\mathcal{O}$ a $\mathcal{O}_p$. Aplicando la proposición 4.1.5 y el teorema de Bezout a las curvas lisas $E$ y $E_p$ tenemos

$$r_p(P * Q) = r_p(P) * r_p(Q)$$

ya que

$$I_{P*Q}(L, E) = I_{r_p(P)*r_p(Q)}(L_p, E_p) = 1.$$

Entonces por la definición de la suma $\oplus$

$$\begin{aligned} r_p(P \oplus Q) &= r_p(\mathcal{O} * (P * Q)) = r_p(\mathcal{O}) * r_p(P * Q) \\ &= \mathcal{O}_p * (r_p(P) * r_p(Q)) = r_p(P) \oplus_p r_p(Q). \end{aligned}$$

Por lo tanto $r_p$ es un homomorfismo de grupos.

□

### 4.1.2 Filtración $p$-ádica.

Fijemos una curva elíptica $E$ definida sobre $\mathbb{Z}$. Con el objeto de conseguir todos o casi todos los puntos de torsión de $E$, es natural trabajar con coordenadas $[x, y, 1]$, quitar denominadores y ver qué ocurre. La dificultad con este camino es que no es fácil sacar partido de la hipótesis de que $[x, y, 1]$ es un punto de torsión. La idea ingeniosa es usar coordenadas $[x, 1, z]$. La proposición 4.1.6 nos dice que

$$r_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p) \text{ es un homomorfismo de grupos si } p \nmid \Delta.$$

En las coordenadas $[x, 1, z]$ , las propiedades de los subgrupos y las de los homomorfismos $r_p$ juegan un papel más visible. Cuando $p \nmid \Delta$, se tiene

$$Ker(r_p) = \{[x, y, z] \in E(\mathbb{Q}) : r_p(x, y, z) = [0, 1, 0]\}.$$

Si $[x, y, z] \in Ker(r_p)$, entonces $y \neq 0$. Por lo tanto normalizando podemos tomar $y = 1$. Los elementos $[x, 1, z] \in E(\mathbb{Q})$ tales que $[x, 1, z] \in Ker(r_p)$ son aquellos para los que

$$|x|_p < 1 \qquad \text{y} \qquad |z|_p < 1.$$

En esta sección vamos a estudiar el conjunto

$$E^{(1)}(\mathbb{Q}) := \{[x, 1, z] \in E(\mathbb{Q}) : |x|_p < 1 \text{ y } |z|_p < 1\},$$

pero sin la hipótesis $p \nmid \Delta$. Es decir, si $p \nmid \Delta$ entonces

$$E^{(1)}(\mathbb{Q}) = Ker(r_p).$$

**Lema 4.1.7** *Sea $[x, 1, z] \in E(\mathbb{Q})$.*

$$Si\ |z|_p < 1 \Longrightarrow |x|_p < 1 \quad y \quad |z|_p = |x|_p^3.$$

*Demostración*: Sea $E(\mathbb{Q})$ una curva elíptica dada por

$$y^2z = x^3 + Axz^2 + Bz^3 \quad A, B \in \mathbb{Z}.$$

Tomando $y = 1$, la ecuación queda en la forma

$$z = x^3 + Axz^2 + Bz^3. \tag{4.4}$$

Supongamos primero que $|x|_p \geq 1$. El término $x^3$ es el mayor con respecto a la norma $|\cdot|_p$ en el lado derecho de la ecuación (4.4), ya que utilizando las hipótesis $A \in \mathbb{Z}$, $|z|_p < 1$ y $|x|_p \geq 1$ tenemos

$$|Axz^2|_p = |A|_p \cdot |xz^2|_p \leq |xz^2|_p = |x|_p \cdot |z|_p^2 < |x|_p \leq |x|_p^3 = |x^3|_p,$$

$$|Bz^3|_p = |B|_p \cdot |z^3|_p \leq |z^3|_p = |z|_p^3 < 1 \leq |x|_p \leq |x|_p^3 = |x^3|_p.$$

Ahora utilizando la propiedad ultramétrica,

$$|z|_p = |x^3 + Axz^2 + Bz^3|_p = |x^3|_p,$$

ya que

$$|a + b|_p = |a|_p \quad \text{siempre que} \quad |b|_p < |a|_p. \tag{4.5}$$

Esto contradice la hipótesis $|x|_p \geq 1$.

Ahora veamos que si $|z|_p < 1$ entonces $|z|_p = |x|_p^3$. Reescribimos (4.4) en la forma siguiente:

$$x^3 = z - Axz^2 - Bz^3. \tag{4.6}$$

Entonces,

- Si $z = 0$, entonces $x = 0$ y obviamente $|z|_p = |x|_p^3$.
- Si $z \neq 0$, entonces el término $z$ es el mayor en el lado derecho de (4.6) con respecto a $|\cdot|_p$ ya que

$$|Axz^2|_p = |A|_p \cdot |x|_p \cdot |z^2|_p \leq |x|_p \cdot |z|_p^2 < |z|_p,$$

$$|Bz^3|_p = |B|_p \cdot |z^3|_p \leq |z|_p^3 < |z|_p.$$

  Utilizando de nuevo la propiedad (4.5), tenemos $|z|_p = |x^3|_p = |x|_p^3$.

Y esto demuestra el Lema.

□

Análogamente a la definición de $E^{(1)}(\mathbb{Q})$, vamos a definir $E^{(n)}(\mathbb{Q})$ para $n > 1$ de la siguiente forma:

$$E^{(n)}(\mathbb{Q}) := \{[x, 1, z] \in E(\mathbb{Q}) : |z|_p < 1 \text{ y } |x|_p \leq p^{-n}\}.$$

Con el lema 4.1.7 podemos reescribir $E^{(n)}(\mathbb{Q})$,

$$E^{(n)}(\mathbb{Q}) := \{[x,1,z] \in E(\mathbb{Q}) : |z|_p \leq p^{-3n}\}.$$

**Definición.** *Se define la* **filtración $p$-ádica de** $E^{(1)}(\mathbb{Q})$ *como*

$$E^{(1)}(\mathbb{Q}) \supseteq E^{(2)}(\mathbb{Q}) \supseteq \ldots \supseteq E^{(n)}(\mathbb{Q}) \ldots$$

*Y se tiene que*

$$\bigcap_{n=1}^{\infty} E^{(n)}(\mathbb{Q}) = \{[0,1,0]\}.$$

**Proposición 4.1.8** *Los subconjuntos $E^{(n)}(\mathbb{Q})$ de $E(\mathbb{Q})$ son subgrupos. La función $x(P)$ que manda $P = [x,1,z]$ a $x(P) = x$ nos da una aplicación $E^{(n)}(\mathbb{Q}) \longrightarrow p^n\mathbb{Z}_{(p)}$. Además, la composición de esta aplicación con la aplicación cociente*

$$p^n\mathbb{Z}_{(p)} \longrightarrow \frac{p^n\mathbb{Z}_{(p)}}{p^{\alpha n}\mathbb{Z}_{(p)}} \qquad \boxed{\alpha = 2 \text{ ó } 3},$$

*es un homomorfismo de grupos*

$$E^{(n)}(\mathbb{Q}) \longrightarrow \frac{p^n\mathbb{Z}_{(p)}}{p^{\alpha n}\mathbb{Z}_{(p)}},$$

*cuyo núcleo está contenido en $E^{(\alpha n)}(\mathbb{Q})$. Por lo tanto, el homomorfismo*

$$\frac{E^{(n)}(\mathbb{Q})}{E^{(\alpha n)}(\mathbb{Q})} \longrightarrow \frac{p^n\mathbb{Z}_{(p)}}{p^{\alpha n}\mathbb{Z}_{(p)}}$$

*es inyectivo.*

Antes de dar la demostración de esta proposición, observemos que tenemos la siguiente cadena de isomorfismos

$$\frac{p^n\mathbb{Z}_{(p)}}{p^{\alpha n}\mathbb{Z}_{(p)}} \cong \frac{p^n\mathbb{Z}}{p^{\alpha n}\mathbb{Z}} \cong \frac{\mathbb{Z}}{p^{(\alpha-1)n}\mathbb{Z}}.$$

Para el segundo de los isomorfismos, observamos que cada grupo es cíclico y ambos tienen $p^{(\alpha-1)n}$ elementos. Para el primero, consideremos la aplicación inducida por la inclusión

$$\frac{p^n\mathbb{Z}}{p^{\alpha n}\mathbb{Z}} \longrightarrow \frac{p^n\mathbb{Z}_{(p)}}{p^{\alpha n}\mathbb{Z}_{(p)}}.$$

Es inyectiva ya que

$$p^n\mathbb{Z} \cap p^{\alpha n}\mathbb{Z}_{(p)} \subseteq p^{\alpha n}\mathbb{Z}.$$

Nos falta ver que es sobreyectiva. Sea $p^n\frac{u}{v} \in p^n\mathbb{Z}_{(p)}$, elegimos $a, b \in \mathbb{Z}$ de forma que

$$av + bp^{(\alpha-1)n} = u. \tag{4.7}$$

Esto se puede hacer ya que $(v,p)=1$. Por (4.7),

$$\frac{p^n u}{v} = p^n a + \frac{p^{\alpha n} b}{v},$$

y esto muestra que para cualquier elemento $\left[p^n \frac{u}{v}\right] \in p^n\mathbb{Z}_{(p)}\Big/p^{\alpha n}\mathbb{Z}_{(p)}$, existe $[p^n a] \in p^n\mathbb{Z}\Big/p^{\alpha n}\mathbb{Z}$ de tal forma que nuestra aplicación manda $[p^n a]$ en $\left[p^n \frac{u}{v}\right]$. Y esto muestra la sobreyectividad.

Ahora veamos un lema que nos será útil en la demostración de la proposición 4.1.8.

**Lema 4.1.9** *Sea $L$ una recta que corta a $E(\mathbb{Q})$ en los puntos $P_i = [x_i, 1, z_i]$,$i = 1,2,3$.*

$$\textit{Si } P_1 \textit{ y } P_2 \in E^{(n)}(\mathbb{Q}) \Longrightarrow P_3 \in E^{(n)}(\mathbb{Q}).$$

*Además,*

$$|x_1 + x_2 + x_3|_p \leq p^{-5n}.$$

*Demostración*: La primera parte de la demostración mostrará que la recta $L$ es de la forma

$$z = mx + b,$$

y daremos una cota para la pendiente $m$. Tenemos que los puntos $P_1, P_2$ y $P_3$ satisfacen la ecuación (4.4). Vamos a diferenciar dos casos:

1. $P_1 \neq P_2$. Sustituyendo los puntos $P_1$ y $P_2$ en la ecuación (4.4) y restando los dos resultados obtenemos

$$z_1 - z_2 = x_1^3 - x_2^3 + A(x_1 z_1^2 - x_2 z_2^2) + B(z_1^3 - z_2^3). \tag{4.8}$$

Cada término de (4.8) es de la forma:

$$\begin{aligned} x_1^s z_1^t - x_2^s z_2^t = & \ (x_1^s - x_2^s) z_1^t + x_2^s (z_1^t - z_2^t) = \\ = & \ (x_1 - x_2)(x_1^{s-1} + x_1^{s-2} x_2 + \ldots + x_1 x_2^{s-2} + x_2^{s-1}) z_1^t + \\ & (z_1 - z_2)(z_1^{t-1} + z_1^{t-2} z_2 + \ldots + z_1 z_2^{t-2} + z_2^{t-1}) x_2^s. \end{aligned} \tag{4.9}$$

Vemos que todos los términos de (4.4) excepto $z$ y $x^3$, tienen $s + 3t \geq 7$.

Tomando $P_1$ y $P_2$ en $E^{(n)}(\mathbb{Q})$, obtenemos

$$\begin{aligned} & |(x_1 - x_2)(x_1^{s-1} + x_1^{s-2} x_2 + \ldots + x_1 x_2^{s-2} + x_2^{s-1}) z_1^t|_p \leq \\ & \leq |x_1 - x_2|_p p^{-n(s-1)} p^{-3nt} \leq p^{-3n} |x_1 - x_2|_p \qquad \text{si } s > 0. \end{aligned}$$

Y análogamente,

$$\begin{aligned} & |(z_1 - z_2)(z_1^{t-1} + z_1^{t-2} z_2 + \ldots + z_1 z_2^{t-2} + z_2^{t-1}) x_2^s|_p \leq \\ & \leq [z_1 - z_2]_p p^{-3n(t-1)} p^{-ns} \leq p^{-n} |z_1 - z_2|_p \qquad \text{si } t > 0. \end{aligned}$$

Utilizando (4.9) tenemos

$$\begin{aligned} x_1^3 - x_2^3 &= (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) \\ x_1z_1^2 - x_2z_2^2 &= (x_1 - x_2)z_1^2 + x_2(z_1 + z_2)(z_1 - z_2) \\ z_1^3 - z_2^3 &= (z_1 - z_2)(z_1^2 + z_1z_2 + z_2^2). \end{aligned}$$

Sustituyendo estos términos en (4.8) tenemos

$$\begin{aligned} z_1 - z_2 = \; & (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) + A(x_1 - x_2)z_1^2 + \\ & + Ax_2(z_1 + z_2)(z_1 - z_2) + B(z_1 - z_2)(z_1^2 + z_1z_2 + z_2^2). \end{aligned}$$

Reordenando los términos

$$(z_1-z_2)(1-Ax_2(z_1+z_2)-B(z_1^2+z_1z_2+z_2^2)) = (x_1-x_2)(x_1^2+x_1x_2+x_2^2+Az_1^2)$$

Por lo que podemos poner

$$(z_1 - z_2)(1 + u) = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 + v), \tag{4.10}$$

con $|u|_p \leq p^n$ y $|v|_p \leq p^{-3n}$. En particular, como $|u|_p < 1$ se tiene $|u+1|_p = 1$.

Si $x_1 = x_2$ entonces tendríamos $z_1 = z_2$, pero esto no se puede dar ya que $P_1 \neq P_2$. Por lo tanto $x_1 \neq x_2$ y esto nos muestra que la recta que une $P_1$ y $P_2$ es de la forma

$$z = mx + b.$$

Usando (4.10) y que $x_1 \neq x_2$, la pendiente $m$ está dada por

$$m = \frac{z_1 - z_2}{x_1 - x_2} = \frac{x_1^2 + x_1x_2 + x_2^2 + v}{1 + u}.$$

Entonces,

$$\begin{aligned} |m|_p = \; & \left| \frac{x_1^2 + x_1x_2 + x_2^2 + v}{1 + u} \right|_p = |x_1^2 + x_1x_2 + x_2^2 + v|_p \leq \\ \leq \; & max\{p^{-2n}, p^{-3n}\} = p^{-2n}. \end{aligned}$$

2. $P_1 = P_2$. La recta en cuestión es la tangente a $E$ en $P$. Vamos a calcularla derivando implícitamente la ecuación (4.4) y evaluando en el punto $[x, 1, z] = [x_1, 1, z_1]$:

$$(1 - 2Ax_1z_1 - 3Bz_1^2)dz = (3x_1^2 + Az_1^2)dx.$$

El coeficiente de $dz$ es de la forma $1 + u'$ con $|u'|_p < 1$. Por lo tanto $\frac{dz}{dx}$ es finito. Y con ello la recta tangente es de la forma

$$z = mx + b,$$

con la pendiente dada por

$$m = \frac{3x_1^2 + Az_1^2}{1 + u'}.$$

Entonces,

$$|m|_p = \left|\frac{3x_1^2 + Az_1^2}{1+u'}\right|_p = |3x_1^2 + Az_1^2|_p \leq max\{p^{-2n}, p^{-6n}\} \leq p^{-2n}.$$

En ambos casos hemos obtenido

$$|m|_p \leq p^{-2n}. \tag{4.11}$$

Como $z_1 = mx_1 + b$, tenemos $b = z_1 - mx_1$ y por lo tanto

$$|b|_p \leq p^{-3n}. \tag{4.12}$$

Los tres puntos $P_1, P_2$ y $P_3$ satisfacen la ecuación $z = mx + b$ y también (4.4) contando multiplicidades. Por lo que si sustituimos $z = mx + b$ en (4.4) obtenemos

$$(mx + b) = x^3 + Ax(mx + b)^2 + B(mx + b)^3$$

cuyas raíces, contando multiplicidades, son $x_1, x_2$ y $x_3$. Entonces $x_1 + x_2 + x_3$ debe ser igual, salvo signo, al cociente del coeficiente de $x^2$ entre el de $x^3$, es decir,

$$x_1 + x_2 + x_3 = \frac{2Amb + 3Bm^2b}{1 + Am^2 + Bm^3}.$$

Usando la desigualdad (4.11) tenemos que el denominador de $x_1 + x_2 + x_3$ tiene norma $p$-ádica igual a 1. Ahora utilizando de nuevo (4.11) y (4.12) obtenemos

$$|x_1 + x_2 + x_3|_p \leq max\{|mb|_p, |m^2b|_p\} = |mb|_p \leq p^{-2n}p^{-3n} = p^{-5n},$$

como queríamos. De $|x_1|_p \leq p^{-n}$ y $|x_2|_p \leq p^{-n}$ deducimos $|x_3|_p \leq p^{-n}$. Y como $z_3 = mx_3 + b$, obtenemos $|z_3|_p \leq p^{-3n}$. Por lo tanto $P_3 \in E^{(n)}(\mathbb{Q})$.

□

*Demostración de la proposición 4.1.8*: Si $P_1$ y $P_2$ pertenecen a $E^{(n)}(\mathbb{Q})$, entonces el Lema 4.1.9 nos dice que $P_3 = P_1 * P_2 \in E^{(n)}(\mathbb{Q})$. Como $\mathcal{O} \in E^{(n)}(\mathbb{Q})$, entonces $\mathcal{O} * (P_1 * P_2) = P_1 \oplus P_2 \in E^{(n)}(\mathbb{Q})$. Además $\mathcal{O} * P_1 = \ominus P_1 \in E^{(n)}(\mathbb{Q})$. Por lo tanto $E^{(n)}(\mathbb{Q})$ es subgrupo de $E(\mathbb{Q})$.

Si $P \in E^{(n)}(\mathbb{Q})$ y $x = x(P)$, entonces $|x|_p \leq p^{-n}$. Por lo tanto,

$$|p^{-n}x|_p = |p^{-n}|_p \cdot |x|_p = p^n|x|_p \leq 1,$$

y con esto,

$$p^{-n}x \in \mathbb{Z}_{(p)} \Longrightarrow x \in p^n\mathbb{Z}_{(p)}.$$

Así hemos visto que tenemos una aplicación

$$\begin{array}{rcl} E^{(n)}(\mathbb{Q}) & \longrightarrow & p^n\mathbb{Z}_{(p)} \\ P & \longmapsto & x(P) \end{array}$$

Sea $P_3 = P_1 * P_2$. El lema 4.1.9 nos dice que

$$x(P_1) + x(P_2) + x(P_3) \in p^{3n}\mathbb{Z}_{(p)} \subset p^{2n}\mathbb{Z}_{(p)}. \tag{4.13}$$

Si $P_3 = [x_3, 1, z_3]$, entonces $\mathcal{O} * P_3 = \ominus P_3 = [-x_3, 1, -z_3]$. Por la definición de $P_3$,

$$x(P_1 \oplus P_2) = x(\ominus P_3) = -x_3,$$

es decir,

$$x(P_1 \oplus P_2) + x(P_3) = -x_3 + x_3 = 0 \in p^{3n}\mathbb{Z}_{(p)} \subset p^{2n}\mathbb{Z}_{(p)}. \tag{4.14}$$

Por lo tanto uniendo (4.13) y (4.14) obtenemos:

$$x(P_1 \oplus P_2) \equiv x(P_1) + x(P_2)\, mod p^{\alpha n}\mathbb{Z}_{(p)} \quad \text{con } \alpha = 2 \text{ ó } 3.$$

Así que la composición

$$\begin{array}{ccccc} E^{(n)}(\mathbb{Q}) & \longrightarrow & p^n\mathbb{Z}_{(p)} & \longrightarrow & p^n\mathbb{Z}_{(p)} \Big/ p^{\alpha n}\mathbb{Z}_{(p)} \\ P & \longmapsto & x(P) & \longmapsto & x(P) + p^{\alpha n}\mathbb{Z}_{(p)} \end{array}$$

es un homomorfismo.

Si $P = [x, 1, z] \in E^{(n)}(\mathbb{Q})$ pertenece al núcleo del homomorfismo anterior, entonces $x = x(P) \in p^{\alpha n}\mathbb{Z}_{(p)}$ y $|z|_p < 1$. Entonces $|x|_p \leq p^{-\alpha n}$, y por lo tanto

$$P \in E^{(\alpha n)}(\mathbb{Q}) \qquad \alpha = 2 \text{ ó } 3.$$

Esto completa la demostración.

□

**Proposición 4.1.10** *Para todo primo p, se tiene que*

$$E(\mathbb{Q})_{tors} \cap E^{(1)}(\mathbb{Q}) = \mathcal{O}.$$

*Demostración*: Fijemos un primo $p$. Si $E(\mathbb{Q})_{tors} \cap E^{(1)}(\mathbb{Q}) \neq \mathcal{O}$, la intersección contiene un elemento $P \neq \mathcal{O}$ de orden algún primo $q$. Como $\bigcap_{n=1}^{\infty} E^{(n)}(\mathbb{Q}) = \mathcal{O}$, podemos encontrar $n$ tal que

$$P \in E^{(n)}(\mathbb{Q}) \smallsetminus E^{(n+1)}(\mathbb{Q}).$$

Por hipótesis tenemos $[q]P = \mathcal{O}$ y por la proposición 4.1.8 la aplicación

$$\begin{array}{ccc} \dfrac{E^{(n)}(\mathbb{Q})}{E^{(3n)}(\mathbb{Q})} & \longrightarrow & \dfrac{p^n\mathbb{Z}_{(p)}}{p^{3n}\mathbb{Z}_{(p)}} \\ P & \longmapsto & x(P) + p^{3n}\mathbb{Z}_{(p)} \end{array} \tag{4.15}$$

es un homomorfismo inyectivo. Entonces,

$$q \cdot x(P) \in p^{3n}\mathbb{Z}_{(p)}.$$

Ahora, si $p \neq q$, entonces $x(P) \in p^{3n}\mathbb{Z}_{(p)} \subset p^{2n}\mathbb{Z}_{(p)}$. Mientras que si $p = q$, entonces $x(P) \in p^{3n-1}\mathbb{Z}_{(p)} \subset p^{2n}\mathbb{Z}_{(p)}$. En ambos casos, la inyectividad del homomorfismo definido por la proposición 4.1.8 nos dice que

$$P \in E^{(2n)}(\mathbb{Q}) \subseteq E^{(n+1)}(\mathbb{Q}),$$

contradicción con la hipótesis $P \in E^{(n)}(\mathbb{Q}) \setminus E^{(n+1)}(\mathbb{Q})$.

□

**Corolario.** *Sea $E$ una curva elíptica definida por*

$$zy^2 = x^3 + Axz^2 + Bz^3 \qquad A, B \in \mathbb{Z}.$$

*Sea $r_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p)$. Entonces,*

$$\text{si } p \nmid \Delta \Longrightarrow r_p|_{E(\mathbb{Q})_{tors}} : E(\mathbb{Q})_{tors} \longrightarrow E_p(\mathbb{F}_p) \text{ es inyectiva.}$$

*Demostración*: Cuando $p \nmid \Delta$ se tiene que

$$Ker(r_p) = E^{(1)}(\mathbb{Q})$$

y por la proposición 4.1.10

$$E(\mathbb{Q})_{tors} \cap E^{(1)}(\mathbb{Q}) = \mathcal{O}.$$

Por lo tanto la restricción de $r_p$ a $E(\mathbb{Q})_{tors}$ es un homomorfismo inyectivo.

□

### 4.1.3 Demostración del Teorema de Nagell-Lutz.

Sea $E$ una curva elíptica definida por

$$zy^2 = x^3 + Axz^2 + Bz^3 \qquad A, B \in \mathbb{Z}.$$

(i) Si $P = [x(P), y(P), 1] \in E(\mathbb{Q})_{tors} \Longrightarrow x(P), y(P) \in \mathbb{Z}$.

Primero supongamos que $y(P) \neq 0$. Entonces $[x(P), y(P), 1] = [X, 1, Z]$, donde $X = \dfrac{x(P)}{y(P)}$ y $Z = \dfrac{1}{y(P)}$. Fijado un primo $p$, la proposición 4.1.10 nos dice que el punto de torsión $[X, 1, Z] \notin E^{(1)}(\mathbb{Q})$, luego $|Z|_p \geq 1$. Por tanto,

$$|y(P)|_p = \left|\frac{1}{Z}\right|_p \leq 1.$$

Pero esta condición ocurre para todo primo $p$, por lo tanto $y(P) \in \mathbb{Z}$.

En el caso $y(P) = 0$ también tenemos que $y(P) \in \mathbb{Z}$.

Ahora sustituyendo $y(P) \in \mathbb{Z}$ en la ecuación

$$zy^2 = x^3 + Axz^2 + Bz^3 \qquad A, B \in \mathbb{Z},$$

vemos que $x(P)$ es la solución de una ecuación polinómica cúbica y mónica con coeficientes enteros , por lo que las raíces para esta ecuación son enteras. Por lo tanto $x(P) \in \mathbb{Z}$.

(ii) Si $P = [x(P), y(P), 1] \in E(\mathbb{Q})_{tors}$, entonces $y(P) = 0$ o bien $y(P) \neq 0$ e $y(P)^2$ divide a $d = -(4A^3 + 27B^2)$. Veámoslo:

Sea $P = [x, y, 1]$. La fórmula del doble de un punto en $E(\mathbb{Q})$ nos da

$$x([2]P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}.$$

Reescribiendo esta última ecuación como

$$x([2]P) = \frac{\phi(x)}{4\varphi(x)} \qquad \text{donde } \varphi(x) = y^2,$$

tenemos

$$\phi(x) = 4y^2\, x([2]P). \tag{4.16}$$

Por el apartado (i), $x, x([2]P)$ e $y^2 \in \mathbb{Z}$; esto junto con la igualdad (4.16), nos dice que $\phi(x) \in \mathbb{Z}$ y que $y^2 \,|\, \phi(x)$. Por tanto,

$$y^2 \,|\, \phi(x) \qquad \text{e} \qquad y^2 \,|\, \varphi(x).$$

Haciendo cálculos se llega a

$$(3x^2 + 4A)\phi(x) - (3x^3 - 5Ax - 27B)\varphi(x) = 4A^3 + 27B^2,$$

y como $y^2 \,|\, \phi(x)$ e $y^2 \,|\, \varphi(x)$ se tiene

$$y^2 \,|\, 4A^3 + 27B^2.$$

Así concluimos la demostración del Teorema de Nagell-Lutz.

□

## 4.2 Casos particulares y el Teorema de Mazur.

En esta sección veremos que como consecuencia del Teorema de Nagell-Lutz, dada una curva elíptica $E$ definida sobre $\mathbb{Q}$, siempre podemos determinar completamente el subgrupo de torsión $E(\mathbb{Q})_{tors}$. El algoritmo consiste en tomar la curva en su ecuación normal de Weierstrass y considerar divisores cuadrados $y^2$ de $d$ para así darnos candidatos a $y(P) = y$, y con estos conseguir el correspondiente entero $x$ tal que $(x, y)$ es una solución entera de

$$y^2 = x^3 + Ax + B.$$

Sólo hay un número finito de posibilidades, y así conseguiremos una cota para $|E(\mathbb{Q})_{tors}|$. Para cada solución entera $(x, y)$ hay que comprobar que es un punto de torsión y para ello hay que ver que el orden de $(x, y)$ es finito. Este algoritmo es a menudo tedioso, es más eficiente usar el corolario de la proposición 4.1.10, para así eliminar posibilidades. En §4.2.1 veremos algunos ejemplos que nos ilustraran este método para hallar $E(\mathbb{Q})_{tors}$. Además veremos algunos casos particulares de subgrupos de torsión en familias de curvas elípticas. También discutiremos las posibles formas que puede tener $E(\mathbb{Q})_{tors}$ para una curva elíptica $E$ cualquiera. Para ello enunciaremos un resultado central en el estudio de curvas elípticas definidas sobre $\mathbb{Q}$. Dicho resultado es el *Teorema de Mazur*, que es un teorema de clasificación de $E(\mathbb{Q})_{tors}$.

### 4.2.1 Casos particulares.

**Ejemplo 4.2.1** Sea $E$ la curva elíptica definida por

$$E : y^2 = x^3 - 4.$$

Entonces

$$d = -(4A^3 + 27B2) = -3^3 \cdot 2^4.$$

La posibilidad $y = 0$ no se da, ya que la ecuación $x^3 - 4 = 0$ no tiene soluciones enteras. Por lo tanto $E$ no tiene puntos de 2-torsión. Ahora buscamos los enteros $y$ tales que $y^2 \mid d$, entonces

$$y \in \{\pm 1, \pm 2, \pm 4, \pm 3, \pm 6, \pm 12\}.$$

Comprobamos que los únicos posibles puntos de torsión son $P_\pm = (2, \pm 2) \in E(\mathbb{Q})$. Veamos si $P_\pm$ tiene orden finito

$$x(P_\pm) = 2, \qquad x([2]P_\pm) = 5 \qquad x([4]P_\pm) = \frac{5 \cdot 157}{4 \cdot 11^2} \notin \mathbb{Z}.$$

Entonces $P_\pm \notin E(\mathbb{Q})_{tors}$. Así obtenemos

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}\}.$$

Con este ejemplo vemos que la parte de torsión de una curva elíptica puede ser el elemento neutro.

En el siguiente ejemplo vamos a utilizar la reducción módulo un primo $p$ para hallar el subgrupo de torsión.

**Ejemplo 4.2.2** Sea $E$ la curva elíptica definida por la forma normal de Weierstrass

$$y^2 = x^3 - 43x + 166.$$

Vamos a buscar la lista completa de canditos a puntos de torsión usando el Teorema de Nagell-Lutz. Se tiene

$$d = -425984 = -2^{15} \cdot 13.$$

Por lo tanto, usando el apartado (ii) del Teorema de Nagell-Lutz, tenemos que si $P = [x(P), y(P), 1] \in E(\mathbb{Q})_{tors}$ entonces

$$y(P) \in \{0, \pm 1, \pm 2, \pm 4, \pm 8, \pm 16, \pm 32, \pm 64, \pm 128\}.$$

Realizando una serie de cálculos comprobamos que las únicas posibilidades son

$$\{(3, \pm 8), (-5, \pm 16), (11, \pm 32)\} \cup \{\mathcal{O}\}.$$

Por otra parte, $3 \not| d$, por lo tanto el corolario de la proposición 4.1.10 nos asegura que la aplicación

$$r_3 : E(\mathbb{Q})_{tors} \longrightarrow E_3(\mathbb{F}_3)$$

es un homomorfismo inyectivo, en otras palabras, $E$ tiene buena reducción módulo 3. Calculamos los puntos de $E_3(\mathbb{F}_3)$ y obtenemos

$$E_3(\mathbb{F}_3) = \{\mathcal{O}_3, (\pm 1, 1), (0, 1), (\pm 1, 2), (0, 2)\},$$

por lo que

$$|E_3(\mathbb{F}_3)| = 7.$$

Ahora usando la fórmula de $x([2]P)$ para el punto $P = (3, 8)$ obtenemos

$$x(P) = 3, \qquad x([2]P) = -5, \qquad x([4]P) = 11, \qquad x([8]P) = 3;$$

y, por lo tanto, $[8]P = \pm P$. Es decir que $P$ es un punto de torsión de orden 7 ó 9 (no tienen orden 3 ya que $x(P) \neq x([2]P)$). Como $\#E_3(\mathbb{F}_3) = 7$ y $r_3 : E(\mathbb{Q})_{tors} \longrightarrow E_3(\mathbb{F}_3)$ es inyectiva, la única posibilidad es que $P = (3, 8)$ tenga orden 7. Entonces concluimos que $E(\mathbb{Q})_{tors}$ es un grupo cíclico de orden 7, cuyos puntos son

$$\{(3, \pm 8), (-5, \pm 16), (11, \pm 32)\} \cup \{\mathcal{O}\}.$$

Hemos obtenido

$$E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/7\mathbb{Z}.$$

En el siguiente ejemplo vamos a hallar $E(\mathbb{Q})_{tors}$ de dos formas distintas. La primera usando el Teorema de Nagell-Lutz y en la segunda mediante reducción $p$-ádica, y veremos que no es suficiente con reducir en un sólo primo.

**Ejemplo 4.2.3** Tenemos la curva elíptica $E$ dada por

$$E : y^2 = x^3 + x.$$

Entonces $d = -4$, por lo que los únicos posibles puntos de torsión tendrán coordenadas $y = 0$ ó $y = \pm 2$. Para $y = 0$ obtenemos $P = (0, 0)$, que es un punto de 2-torsión. Mientras que observamos que $E(\mathbb{Q})$ no contiene puntos con abscisa igual a $\pm 2$. Por lo tanto,

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0, 0)\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

También podemos calcular $E(\mathbb{Q})_{tors}$ sin usar el Teorema de Nagell-Lutz, utilizando reducción módulo $p$, con $p$ un primo adecuado. Calculando obtenemos

$$\#E_3(\mathbb{F}_3) = 4, \qquad \#E_5(\mathbb{F}_5) = 4, \qquad \#E_7(\mathbb{F}_7) = 8.$$

De hecho se tiene que 4 divide a $\#E_p(\mathbb{F}_p)$ $\forall p \geq 3$. Para los casos $p = 3, 5$ obtenemos

$$E_3(\mathbb{F}_3) = \{\mathcal{O}_3, (0, 0), (2, 1), (2, 2)\} \simeq \mathbb{Z}/4\mathbb{Z},$$

$$E_5(\mathbb{F}_5) = \{\mathcal{O}_5, (0, 0), (2, 0), (3, 0)\} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Entonces, como $r_p : E(\mathbb{Q})_{tors} \longrightarrow E_p(\mathbb{F}_p)$ es inyectiva para todo primo $p \neq 2$,

$$E(\mathbb{Q})_{tors} = \begin{cases} \{\mathcal{O}\} \\ \text{ó} \\ \mathbb{Z}/2\mathbb{Z} \end{cases},$$

y como $(0,0) \in E(\mathbb{Q})_{tors}$, se obtiene

$$E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z}.$$

Por último, el siguiente ejemplo muestra que $E(\mathbb{Q})_{tors}$ puede ser relativamente grande y no ser cíclico.

**Ejemplo 4.2.4** Sea $E$ la curva elíptica definida por

$$y^2 = x^3 + 337x^2 + 20736x.$$

Como $E$ no está dada en su forma normal de Weierstrass no podemos utilizar directamente el Teorema de Nagell-Lutz. Pero cambiar a la forma normal es un isomorfismo sobre $\mathbb{Q}$, y por lo tanto $E(\mathbb{Q})_{tors}$ no varía. Usando las fórmulas de (1.5) a (1.11) y simplificando, obtenemos

$$y^2 = x^3 + Ax + B,$$

con

$$\begin{cases} A = -3^3 \cdot 4 \cdot 821776, \\ \\ B = 3^3 \cdot 4^3 \cdot 218451488. \end{cases}$$

Por tanto,

$$d = 4A^3 + 27B^2 = 2^{20} \cdot 3^{10} \cdot 17 \cdot 19 \cdot 181 \cdot 4283 \cdot 67789.$$

El Teorema de Nagell-Lutz nos dice que

$$y \in \{2^k \cdot 3^j : k = 0, \ldots, 10; j = 0, \ldots, 5\} \cup \{0\}.$$

Sustituyendo los valores de $y$ en la ecuación

$$x^3 + Ax + B - y^2 = 0, \tag{4.17}$$

obtenemos los valores de $x$. El Teorema de Nagell-Lutz nos asegura que para que un punto $P = (x, y)$ sea de torsión es necesario que $x, y \in \mathbb{Z}$. De las soluciones enteras de (4.17), calculamos cúales de ellas corresponden a puntos de torsión. Y

obtenemos que los puntos de torsión son, junto con su orden:

| Punto | orden |
|---|---|
| $(-256, 0)$ | 2 |
| $(-216, -1080)$ | 8 |
| $(-216, 1080)$ | 8 |
| $(-144, -1008)$ | 4 |
| $(-144, 1008)$ | 4 |
| $(-96, -480)$ | 8 |
| $(-96, 480)$ | 8 |
| $(-81, 0)$ | 2 |
| $(0, 0)$ | 2 |
| $(24, -840)$ | 8 |
| $(24, 840)$ | 8 |
| $(144, -3600)$ | 4 |
| $(144, 3600)$ | 4 |
| $(864, -30240)$ | 8 |
| $(864, 30240)$ | 8 |
| $\mathcal{O}$ | 1 |

Así obtenemos

$$|E(\mathbb{Q})_{tors}| = 16,$$

y como de los 16 puntos anteriores tenemos que el orden máximo es 8, sólo puede ser

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

### 4.2.2 Subgrupo de torsión en algunas familias de curvas elípticas.

En este apartado enunciaremos dos teoremas que nos darán el subgrupo de torsión para un número infinito de curvas elípticas. Las demostraciones de estos teoremas, que enunciaremos a continuación, se basan en el Teorema de Dirichlet de los primos en una progresión aritmética.

**Teorema de Dirichlet de los primos en una progresión aritmética.** *Sean $a, b \in \mathbb{Z}$ tales que $a > 0$ y $(a, b) = 1$. Entonces existen infinitos primos en la progresión aritmética*

$$an + b, \qquad n \in \mathbb{N}.$$

*Demostración*: Ver [C-C], Capítulo IX, Sección 9.4.

Ahora enunciamos los teoremas que nos clasifican el subgrupo de torsión de algunas familias de curvas elípticas.

**Teorema 4.2.1** *Sea $E$ una curva elíptica dada por*

$$y^2 = x^3 + Ax \qquad A \in \mathbb{Z},$$

*y supongamos que $A$ no tiene potencias cuartas. Entonces:*

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{si } -A \text{ es un cuadrado en } \mathbb{Z}, \\ \mathbb{Z}/4\mathbb{Z} & \text{si } A = 4, \\ \mathbb{Z}/2\mathbb{Z} & \text{en otro caso.} \end{cases}$$

Para la demostración de este teorema, necesitamos el siguiente lema:

**Lema 4.2.2** *Sea $E_p$ la reducción de la curva $y^2 = x^3 + Ax$ sobre $\mathbb{F}_p$, y supongamos que $p \nmid \Delta$, $p \geq 7$ y $p \equiv 3 \bmod 4$. Entonces,*

$$|E_p(\mathbb{F})| = p + 1.$$

*Demostración:* Primero daremos algunos resultados sobre Residuos Cuadráticos. Para ver un desarrollo mayor de esta teoría ver [C-C]. Sea $p$ un primo impar, se define el **símbolo de Legendre** $\left(\frac{a}{p}\right)$ a la función definida por

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \bmod p, \\ 1 & \text{si } \exists b \text{ tal que } a \equiv b^2 \bmod p, \\ -1 & \text{si } \nexists b \text{ tal que } a \equiv b^2 \bmod p. \end{cases}$$

Se tiene que el símbolo de Legendre es una función completamente multiplicativa, es decir,

$$\left(\frac{m \cdot n}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right) \quad \forall m, n.$$

Además, se tiene

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \bmod 4, \\ -1 & \text{si } p \equiv 3 \bmod 4. \end{cases}$$

Para $q \neq 0$, consideramos el par $\{q, -q\}$. Cuando estos elementos son sustituidos en $x^3 + Ax$, obtenemos $Q = q^3 + Aq$ y $-Q$. Si tenemos $Q = 0$, se tiene que de $\{\alpha, -\alpha\}$ obtenemos los puntos $(\alpha, 0)$ y $(-\alpha, 0)$. Si $Q \neq 0$, tenemos dos posibilidades:

- Si $\left(\frac{Q}{p}\right) = 1$ entonces $\left(\frac{-Q}{p}\right) = -1$. Por lo tanto de $\{\alpha, -\alpha\}$ obtenemos los puntos $(\alpha, \sqrt{Q})$ y $(\alpha, -\sqrt{Q})$.
- Si $\left(\frac{Q}{p}\right) = -1$ entonces $\left(\frac{-Q}{p}\right) = 1$. Por lo tanto de $\{\alpha, -\alpha\}$ obtenemos los puntos $(-\alpha, \sqrt{Q})$ y $(-\alpha, -\sqrt{Q})$.

Por lo tanto, a cada par $\{\alpha, -\alpha\}$ le corresponden dos puntos de $E_p(\mathbb{F}_p)$. Esto es, $|E_p(\mathbb{F}_p \setminus \{0\})| = p - 1$. Para $x = 0$ obtenemos el punto $(0, 0)$, y junto con el punto $\mathcal{O}_p$ obtenemos

$$|E_p(\mathbb{F}_P)| = p + 1.$$

□

*Demostración del Teorema 4.2.1:* El primer paso es mostrar que $|E(\mathbb{Q})_{tors}|$ divide a 4. Por la proposición 4.1.6 y por el corolario de la proposición 4.1.10, para $p$ suficientemente grande, $|E(\mathbb{Q})_{tors}|$ divide a $|E_p(\mathbb{F}_p)|$. Por el lema 4.2.2, $|E(\mathbb{Q})_{tors}|$ divide a $p + 1$ para $p$ suficientemente grande y $p \equiv 3 \bmod 4$.

Veamos que 8 no divide a $|E(\mathbb{Q})_{tors}|$. Por el Teorema de Dirichlet, podemos elegir un primo $p$ tal que $p \equiv 3 \bmod 8$. Si 8 divide a $|E(\mathbb{Q})_{tors}|$, entonces $8 \,|\, (p+1)$. Por otro lado como $p \equiv 3 \bmod 8$, se tiene que $p + 1 \equiv 4 \bmod 8$ y por lo tanto $8 \not| (p + 1)$, en contradicción con lo anterior.

Ahora veamos que 3 no divide a $|E(\mathbb{Q})_{tors}|$. Por el Teorema de Dirichlet, podemos elegir un primo $p$ tal que $p \equiv 7 \bmod 12$. Entonces $p \equiv 3 \bmod 4$. Si 3 divide a $|E(\mathbb{Q})_{tors}|$, entonces $3 \,|\, (p + 1)$. Por otro lado como $p + 1 \equiv 8 \bmod 12$ implica que $p + 1 \equiv 2 \bmod 3$ y por lo tanto $3 \not| (p + 1)$, en contradicción con lo anterior.

Finalmente vamos a ver que no existe $q$ primo impar $> 3$ tal que divida a $|E(\mathbb{Q})_{tors}|$. De nuevo, por el Teorema de Dirichlet, podemos elegir un primo $p$ tal que $p \equiv 3 \bmod 4q$. Entonces $p \equiv 3 \bmod 4$. Si $q$ divide a $|E(\mathbb{Q})_{tors}|$ entonces $q \,|\, (p + 1)$. Pero $p + 1 \equiv 4 \bmod 4q$ implica que $p + 1 \equiv 4 \bmod 4$, y por lo tanto $q \not| (p + 1)$, en contradicción con lo supuesto.

Hemos demostrado que $|E(\mathbb{Q})_{tors}|$ divide a 4. Por lo tanto $E(\mathbb{Q})_{tors}$ contiene a $\mathbb{Z}/2\mathbb{Z} = \{(0, 0), \mathcal{O}_p\}$ como subgrupo, y contiene a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ si y sólo si $x^3 + Ax$ se descompone en monomios sobre $\mathbb{Q}$, es decir, si y sólo si $-A$ es un cuadrado. Por lo tanto la única cuestión es cuándo $(0, 0)$ es el doble de otro punto, y así el grupo de torsión es $\mathbb{Z}/4\mathbb{Z}$ y no $\mathbb{Z}/2\mathbb{Z}$. Podemos ver directamente que para $A = 4$, se tiene $[2](2, 4) = (0, 0)$. Consideramos la ecuación $[2](x, y) = (0, 0)$ para otro $A$ y para $x \neq 0$. Por la fórmula del punto doble tenemos que

$$0 = x^4 - 2Ax^2 + A^2 = (x^2 - A)^2.$$

Esto es, $x^2 = A$. Como $A$ no tiene potencias cuartas, $x$ está libre de cuadrados. Pero $y^2 = x(x^2 + A) = 2x^3$ implica que no existen primos impares que dividan a $x$. Por lo tanto, los únicos casos que nos quedan son $x = \pm 1$ ó $x = \pm 2$. Y se calcula que $x = \pm 2$ y $A = 4$.

□

**Teorema 4.2.3** *Sea $E$ una curva elíptica dada por*

$$y^2 = x^3 + B \qquad B \in \mathbb{Z},$$

*y supongamos que $B$ no tiene potencias sextas. Entonces:*

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/6\mathbb{Z}Z & \text{si } B = 1, \\ \mathbb{Z}/3\mathbb{Z} & \text{si } B = -432 \text{ o si } B \text{ es un cuadrado en } \mathbb{Z} \text{ distinto de } 1, \\ \mathbb{Z}/2\mathbb{Z} & \text{si } B \text{ es un cubo en } \mathbb{Z} \text{ distinto de } 1, \\ \mathcal{O} & \text{en otro caso.} \end{cases}$$

Antes de la demostración veamos un lema:

**Lema 4.2.4** *Sea $E_p$ la reducción de la curva $y^2 = x^3 + B$ sobre $\mathbb{F}_p$, y supongamos que $p \nmid \Delta$, $p \geq 5$ y $p \equiv 2 \bmod 3$. Entonces*

$$|E_p(\mathbb{F})| = p + 1.$$

*Demostración:* Sea $p = 3n + 2$. El grupo multiplicativo $\mathbb{F}_p^*$ tiene orden $p - 1$. Como $3 \nmid (p-1)$, no hay elementos de orden 3. Por lo tanto el homomorfismo

$$\begin{array}{ccc} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ a & \longmapsto & a^3 \end{array}$$

es inyectivo, y también sobreyectivo. Por lo tanto cada elemento de $\mathbb{F}_p$ tiene una única raíz cúbica. Para cada $y \in \mathbb{F}_p$, el elemento $y^2 - B$ tiene una única raíz cúbica. Por lo tanto, obtenemos $p$ puntos de $E_p(\mathbb{F}_p)$. Añadiendo $\mathcal{O}_p$, vemos que $|E_p(\mathbb{F}_p)| = p + 1$.

□

*Demostración del Teorema 4.2.3:* El principal hecho es mostrar que $|E(\mathbb{Q})_{tors}|$ divide a 6. Por la proposición 4.1.6 y por el corolario de la proposición 4.1.10, para $p$ suficientemente grande, $|E(\mathbb{Q})_{tors}|$ divide a $|E_p(\mathbb{F}_p)|$. Por el lema 4.2.4, $|E(\mathbb{Q})_{tors}|$ divide a $p + 1$ para $p$ suficientemente grande y $p \equiv 2 \bmod 3$.

Vamos a ver que 4 no divide a $|E(\mathbb{Q})_{tors}|$. Por el Teorema de Dirichlet, podemos elegir un primo $p$ tal que $p \equiv 5 \bmod 12$. Entonces $p \equiv 2 \bmod 3$. Si 4 divide $|E(\mathbb{Q})_{tors}|$, entonces $4 \,|\, (p+1)$. Pero como $p \equiv 1 \bmod 4$ se tiene que $p+1 \equiv 2 \bmod 4$, esto es, $4 \nmid (p+1)$, contradicción.

Ahora vamos a ver que 9 no divide a $|E(\mathbb{Q})_{tors}|$. Por el Teorema de Dirichlet, podemos elegir un primo $p$ tal que $p \equiv 2 \bmod 9$. Entonces $p \equiv 2 \bmod 3$.

Si 9 divide a $|E(\mathbb{Q})_{tors}|$ entonces $9 \,|\, (p+1)$. Pero $p + 1 \equiv 3 \bmod 9$, es decir $9 \nmid (p+1)$, contradicción.

Por último, veamos que si $q > 3$ es un primo, entonces $q \nmid |E(\mathbb{Q})_{tors}|$. Por el Teorema de Dirichlet, podemos elegir $p \equiv 2 \bmod 3q$. Entonces $p \equiv 2 \bmod 3$. Si $q$

divide a $|E(\mathbb{Q})_{tors}|$ entonces $q \mid (p+1)$. Por otro lado, $p+1 \equiv 3 \bmod 3q$, por tanto $q \nmid (p+1)$, en contradicción con lo anteriormente supuesto.

Hemos demostrado que $|E(\mathbb{Q})_{tors}|$ divide a 6. El grupo de torsión tiene un elemento de orden 2 si y sólo si $B$ es un cubo. Por lo tanto, la unica cuestión es ver cuándo $E(\mathbb{Q})$ contiene elementos de orden 3. Sea $P = (x, y)$ un punto de orden 3, es decir, $[2]P = \ominus P$. Además la coordenada $x$ determina por completo a $P$, ya que $[2]P = P$ es imposible para $P \neq \mathcal{O}_p$. Utilizando la fórmula del doble de un punto tenemos que la condición $[2]P = \ominus P$ se traduce en

$$\frac{x^4 - 8Bx}{4(x^3 + B)} = x,$$

que simplificando se nos queda en

$$x^4 = -4Bx.$$

Una solución es $x = 0$, que da $y^2 = B$; por lo tanto $\mathbb{Z}/3\mathbb{Z}$ es un subgrupo de $E(\mathbb{Q})_{tors}$ si $B$ es un cuadrado. La otra posibilidad es si $x^3 = -4B$, entonces $y^2 = -3B$. Por lo tanto $B < 0$. Como $B$ no tiene potencias sextas entonces $y$ no tiene potencias triples, y esto junto con $x^3 = -4B$, nos dice que los únicos primos que pueden dividir a $B$ son 2 y 3. Y encontramos que entonces se ha de tener $B = -2^4 3^3$. Por lo tanto $\mathbb{Z}/3\mathbb{Z}$ aparece si y sólo si $B$ es un cuadrado ó $B = -2^4 3^3$.

□

### 4.2.3 Teorema de Mazur.

Si tenemos una curva elíptica $E$ definida sobre $\mathbb{Q}$, dada por una ecuación de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}, \tag{4.18}$$

para poder aplicar el Teorema de Nagell-Lutz y así calcular $E(\mathbb{Q})_{tors}$, lo que haremos es poner $E$ en una ecuación normal de Weierstrass

$$y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{Z}. \tag{4.19}$$

Obviamente, el subgrupo de torsión $E(\mathbb{Q})_{tors}$ que obtenemos en (4.19) es isomorfo al de (4.18). La siguiente tabla nos muestra 15 diferentes curvas todas ellas con grupos de torsión distintos.

| $E$ | $E(\mathbb{Q})_{tors}$ |
|---|---|
| $y^2 = x^3 + 2$ | $0$ |
| $y^2 = x^3 + x$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $y^2 = x^3 + 4$ | $\mathbb{Z}/3\mathbb{Z}$ |
| $y^2 = x^3 + 4x$ | $\mathbb{Z}/4\mathbb{Z}$ |
| $y^2 + y = x^3 - x^2$ | $\mathbb{Z}/5\mathbb{Z}$ |
| $y^2 = x^3 + 1$ | $\mathbb{Z}/6\mathbb{Z}$ |
| $y^2 - xy + 2y = x^3 + 2x^2$ | $\mathbb{Z}/7\mathbb{Z}$ |
| $y^2 + 7xy - 6y = x^3 - 6x^2$ | $\mathbb{Z}/8\mathbb{Z}$ |
| $y^2 + 3xy + 6y = x^3 + 6x^2$ | $\mathbb{Z}/9\mathbb{Z}$ |
| $y^2 - 7xy - 36y = x^3 - 18x^2$ | $\mathbb{Z}/10\mathbb{Z}$ |
| $y^2 + 43xy - 210y = x^3 - 210x^2$ | $\mathbb{Z}/12\mathbb{Z}$ |
| $y^2 = x^3 - x$ | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ |
| $y^2 = x^3 + 5x^2 + 4x$ | $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ |
| $y^2 + 5xy - 6y = x^3 - 3x^2$ | $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ |
| $y^2 = x^3 + 337x^2 + 20736x$ | $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ |

Para ver métodos para generar tales ejemplos ver [KNA], Capítulo V, Sección 5.

En estos momentos nos hacemos la siguiente pregunta:

Dado un primo $p$, ¿existe una curva elíptica $E/\mathbb{Q}$ tal que $E(\mathbb{Q})$ contiene un punto de orden $p$?

La respuesta en general es NO. Por ejemplo, $E(\mathbb{Q})$ no contiene nunca puntos de orden 11. Observamos que esto está en consonancia con la tabla anterior, ya que ninguna de las curvas tiene puntos de orden 11. Además resulta que los únicos subgrupos de torsión de una curva elíptica definida sobre $\mathbb{Q}$ son los que aparecen en la tabla anterior. Esta afirmación nos la da el siguiente teorema central en el estudio de las curvas elípticas definidas sobre $\mathbb{Q}$.

**Teorema de Mazur.** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$. Entonces el subgrupo de torsión $E(\mathbb{Q})_{tors}$, es uno de los siguientes 15 grupos:*

$$\begin{array}{cc} \mathbb{Z}/N\mathbb{Z} & 1 \leq N \leq 10 \quad \acute{o} \quad N = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} & 1 \leq N \leq 4. \end{array}$$

Este teorema nos da una caracterización definitiva de los subgrupos de torsión de una curva elíptica definida sobre $\mathbb{Q}$. La demostración del Teorema de Mazur queda fuera de los objetivos de este trabajo. Dicha demostración se puede encontrar en [MAZ1] y [MAZ2], dos trabajos de gran trascendencia en el estudio de las curvas elípticas.

## 4.3 Puntos de torsión de curvas elípticas sobre cuerpos de números.

Sea $E$ una curva elíptica definida sobre un cuerpo de números $K$. Una curva elíptica definida sobre $\mathbb{C}$ es isomorfa a un toro[1] obtenido como cociente de $\mathbb{C}$ por un retículo, tenemos que los puntos $\mathbb{C}$-racionales de $E$ son

$$E(\mathbb{C}) \cong \mathbb{T} \cong S^1 \times S^1.$$

Utilizando el homomorfismo de grupos

$$\begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (S^1, \bullet) \\ x & \longmapsto & e^{2\pi i x} \end{array}$$

obtenemos

$$(\mathbb{R}/\mathbb{Z}, +) \cong (S^1, \bullet).$$

Con este último resultado, obtenemos

$$E(\mathbb{C})_{tors} \cong \mathbb{Q}/\mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}.$$

El Teorema de Mordell-Weil establece que $E(K)$ es un grupo abeliano finitamente generado, y como $E(K) \subset E(\mathbb{C})$, se tiene

$$E(K) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \mathbb{Z}^r,$$

con $n_1, n_2, r \in \mathbb{Z}$ tales que $n_1 \,|\, n_2$, $n_1, n_2 > 0$ y $r \geq 0$. Al par $(n_1, n_2)$ lo denominaremos el **tipo de torsión de** $E(K)$ y al entero $r$ se le llama **rango de** $E(K)$.

A continuación enunciaremos y comentaremos los mayores avances que han ido surgiendo desde que Mazur propició la denominada **Conjetura de acotación uniforme**, hasta la demostración hecha por Merel ([MER]) en Febrero de 1996.

**Conjetura de acotación uniforme.** *Para todo entero $d \leq 1$, existe un entero $B(d)$ tal que para todo cuerpo de números $K$ de grado $d$ sobre $\mathbb{Q}$ y para toda curva elíptica $E$ sobre $K$ se tiene*

$$|E(K)_{tors}| < B(d).$$

A esta conjetura tambien se le denomina **Conjetura de acotación uniforme fuerte**, para resaltar que la cota $B(d)$ es uniforme en todos los cuerpos de números de grado $d$. Ya Mazur fue capaz de demostrar esta conjetura para el caso $d = 1$, es decir para $K = \mathbb{Q}$. Además fue capaz de dar una cota explícita. Esta demostración aparació en su artículo de 1977 ([MAZ1]). Es lo que ahora se denomina Teorema de Mazur y que vimos en la sección §4.2.3. Este teorema fue ya conjeturado por Beppo Levi en 1908 y más tarde redescubierto por Ogg. En un trabajo siguiente

[1] Ver [SIL], Capítulo VI, Sección 1.

([MAZ2]), Mazur introdujo una importante simplificación de los argumentos expuestos en [MAZ1]. En estos dos artículos fue donde Mazur introdujo la Conjetura de acotación uniforme. A partir de estos trabajos, pocos progresos fueron hechos en esta conjetura hasta los resultados de Kamienny en 1992 ([KAM]). Este trabajo establece la conjetura para todos los cuerpos cuadráticos $K$. Este artículo intuía que una buena cota debía involucrar sólo el grado de $K$ sobre $\mathbb{Q}$, y no otros invariantes de $K$. De hecho, el argumento de Kamienny es más geométrico que aritmético. En suma, al hablar de el primer progreso serio en la Conjetura de acotación uniforme desde el trabajo de Mazur, la estrategia de Kamienny sugería un método de ataque a la conjetura para cuerpos de números generales de grado $d$.

Ahora introducimos algo de notación. Para $d \geq 1$, sea $K$ un cuerpo de números de grado $d$ y $E$ una curva elíptica definida sobre $K$. Definimos

$$\Phi(d) := \left\{ (n_1, n_2) : \begin{array}{c} \exists \text{K con } [K:\mathbb{Q}] = d \text{ y } \exists E/K \\ \text{tal que } E(K)_{tors} \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \end{array} \right\}$$

y

$$S(d) := \left\{ p \text{ primo } : \begin{array}{c} \exists \text{K con } [K:\mathbb{Q}] = d \text{ y } \exists E/K \\ \text{tal que } p \text{ divide a } |E(K)_{tors}| \end{array} \right\}.$$

Con esta terminología, la Conjetura de acotación uniforme es equivalente a la conjetura siguiente:

**Conjetura.** *Para todo $d \geq 1$, $\Phi(d)$ es un conjunto finito.*

Los resultados de Mazur y Kamienny, anteriormente citados, lo que aseguran es que $\Phi(1)$ y $\Phi(2)$ son finitos. En concreto, el Teorema de Mazur afirma que

$$\Phi(1) = \{(1,m) : 1 \leq m \leq 10\} \cup \{(1,12)\} \cup \{(2,2m) : 1 \leq m \leq 4\}.$$

Además $\Phi(2)$ se determina explícitamente, usando trabajos de Kamienny, Kenku y Momose ([KE-MO]):

$$\begin{aligned} \Phi(2) = \{(1,m) : 1 \leq m \leq 16\} \cup \{(1,18)\} \cup \{(2,2m) : 1 \leq m \leq 6\} \\ \cup \{(3,3m) : 1 \leq m \leq 2\} \cup \{(4,4)\}. \end{aligned}$$

Posteriormente, en 1995, Mazur y Kamienny ([K-M]) demostraron conjuntamente el siguiente teorema:

**Teorema 4.3.1**

*(i) Para $d \leq 8$, el conjunto $\Phi(d)$ es finito.*

*(ii) $\Phi(d)$ es finito $\Longleftrightarrow$ $S(d)$ es finito.*

El apartado (i) de este teorema es una consecuencia de un resultado de Frey (1992), que es a su vez una consecuencia de un teorema de Faltings. Fue probado por Mazur y Kamienny utilizando el criterio de Kamienny. D.Abramovich ([ABR])

llevo el método más lejos aún, y dedujo que $S(d)$ es finito para todo $d \leq 14$ (para $d = 13, 14$ su prueba se basa en cálculo computacional).

Y por último llegamos al artículo de Merel ([MER]), aparecido en 1996. En este artículo, el autor prueba la conjetura de acotación uniforme. Merel demuestra el siguiente teorema:

**Teorema 4.3.2** *Sea $E$ una curva elíptica definida sobre un cuerpo de números $K$ de grado $d > 1$ sobre $\mathbb{Q}$. Si $E(K)$ posee un punto de orden primo $p$, entonces*

$$p < d^{3^{d^2}}.$$

Usando este teorema, Merel, basándose en resultados de Faltings y Frey ([FAL2] y [FRE]), consigue el siguiente corolario, que no es más que la Conjetura de acotación uniforme.

**Corolario.** *Sea un entero $d \geq 1$. Existe un número real $B(d)$ tal que para toda curva elíptica $E$ definida sobre un cuerpo de números $K$ de grado $d$ sobre $\mathbb{Q}$, todo punto de torsión de $E(K)$ es de orden $\leq B(d)$.*

Observamos que este corolario es equivalente a la afirmación siguiente:
"Sólo existe, salvo isomorfismos, un número finito de grupos que son parte de la torsión del grupo de Mordell-Weil de una curva elíptica definida sobre una extensión de $\mathbb{Q}$ de grado $d$."

Posteriormente, Oesterlé mejoró la cota obtenida por Merel reemplazando $d^{3^{d^2}}$ por $(1 + 3^{d/2})^2$.

El anterior corolario de Merel nos asegura la existencia de cotas $B(d)$, pero no de manera efectiva. En efecto, si bien acota los números primos que pueden dividir al orden del grupo $E(K)_{tors}$, no se sabía en la práctica qué potencias de estos primos pueden intervenir. Recientemente, P.Parent ([PAR]) ha dado una demostración efectiva de la Conjetura de acotación uniforme. El resultado es el siguiente:

**Teorema 4.3.3** *Sea $E$ una curva elíptica definida sobre un cuerpo de números $K$ de grado $d$ sobre $\mathbb{Q}$. Si $E(K)$ tiene un punto de orden una potencia $p^n$ de un número primo $p$, se tiene que*

$$p^n \leq \begin{cases} 65 \cdot (3^d - 1) \cdot (2d)^6 & \text{si } p \neq 2, 3, \\ 65 \cdot (5^d - 1) \cdot (2d)^6 & \text{si } p = 3, \\ 129 \cdot (3^d - 1) \cdot (3d)^6 & \text{si } p = 2. \end{cases}$$

Por lo tanto, la conjetura de acotación uniforme está demostrada incluso de forma efectiva. Con lo que el único paso que nos queda por dar es clasificar $E(K)_{tors}$ con $K$ un cuerpo de números de grado $d$, algo que aún se mantiene sin resolver en general.

Por último, enunciaremos una generalización de la conjetura de acotación uniforme que en vez de considerar curvas elípticas definidas sobre cuerpos de números de grado $d$, considera variedades abelianas definidas sobre $\mathbb{Q}$ de dimensión $d$.

**Conjetura.** *Para todo $d \geq 0$, existe un entero $B'(d)$ con la propiedad*

$$|A(\mathbb{Q})_{tors}| < B'(d)$$

*para toda variedad abeliana definida sobre $\mathbb{Q}$ de dimensión $d$.*

Sobre esta conjetura no se sabe casi nada. Para ver algo sobre ella ver [SI].

# Capítulo 5

# Rango del grupo de Mordell.

El Teorema de Mordell nos dice que si $E$ es una curva elíptica definida sobre $\mathbb{Q}$, entonces

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r,$$

donde $E(\mathbb{Q})_{tors}$ es un grupo finito que es fácil de calcular para una curva dada, y $r$ es un entero positivo llamado **rango**. El rango es muy difícil de calcular, incluso para una curva dada.

En primer lugar definiremos la altura canónica asociada a $E(\mathbb{Q})$, con la que definiremos la forma bilineal de Nerón-Tate. Esta forma bilineal nos será de gran utilidad ya que desciende a $E(\mathbb{Q})/E(\mathbb{Q})_{tors} \cong \mathbb{Z}^r$, y aquí es definida positiva. Además nos permitirá ver si un conjunto de elementos de $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ es linealmente independiente en $E(\mathbb{Q})$. Este hecho lo usaremos con frecuencia en el capítulo 7.

En la sección §5.3 obtendremos una fórmula para obtener el rango, aunque por desgracia no será muy útil.

Y por último, en la sección §5.4 obtendremos una cota superior para el rango.

## 5.1 Altura canónica o de Nerón-Tate.

En esta sección vamos a modificar la noción de altura $h_x$, dada en la sección §3.3. A partir de esta altura vamos a construir, en la sección 5.3, una aplicación bilineal definida positiva que desciende a $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$.

**Teorema 5.1.1** *Existe una única función $h : E(\mathbb{Q}) \longrightarrow \mathbb{R}$ satisfaciendo*

*(i)* $h(P) - h_x(P)$ *está acotada.*

*(ii)* $h([2]P) = 4h(P)$.

*Esta función viene dada por la siguiente expresión:*

$$h(P) = \lim_{n\to\infty} \frac{h_x([2^n]P)}{4^n}. \tag{5.1}$$

*Se cumple además que*

1. $h(P) \geq 0$.
2. $h(P) = 0 \iff P$ *tiene orden finito.*
3. $\#\{P : h(P) \leq C\} < \infty$ *para cada* $C \in \mathbb{R}$.

*A la función* $h$ *la llamaremos* **altura canónica** *o* **de Nerón-Tate**.

*Demostración*: Empezamos demostrando la unicidad. Sea $h$ una función satisfaciendo (i) e (ii), con cota $C'$ en (i). Entonces por (i) e (ii) se tiene

$$|4^n h(P) - h_x([2^n]P)| = |h([2^n]P) - h_x([2^n]P)| \leq C',$$

esto es,

$$\left| h(P) - \frac{h_x([2^n]P)}{4^n} \right| \leq \frac{C'}{4^n}.$$

Por tanto $h$ debe de estar dada por (5.1).

Para la existencia, vamos a probar que $\left\{ \dfrac{h_x([2^n]P)}{4^n} \right\}_{n\in\mathbb{N}}$ es de Cauchy. Por la proposición 3.3.1, tenemos

$$|h_x([2]Q) - 4h_x(Q)| \leq C''$$

con $C''$ independiente de $Q$. Entonces si $N \geq M \geq 0$ tenemos

$$\begin{aligned} \left| \frac{h_x([2^N]P)}{4^N} - \frac{h_x([2^M]P)}{4^M} \right| &= \left| \sum_{n=M}^{N-1} \left( \frac{h_x([2^{n+1}]P)}{4^{n+1}} - \frac{4h_x([2^n]P)}{4^{n+1}} \right) \right| \leq \\ &\leq \sum_{n=M}^{N-1} \frac{1}{4^{n+1}} |h_x([2^{n+1}]P) - 4h_x([2^n]P)| \leq \\ &\leq \sum_{n=M}^{N-1} \frac{1}{4^{n+1}} C'' \leq C'' \frac{1}{4} \sum_{n=M}^{\infty} \frac{1}{4^n} = \frac{C''}{3} \frac{1}{4^M}, \end{aligned} \tag{5.2}$$

y la parte derecha tiende a 0 cuando $M$ y $N$ tienden a $\infty$. Por tanto, la función $h$ de (5.1 ) está bien definida, y es evidente que satisface (ii).

Haciendo tender $N$ a $\infty$ y tomando $M = 0$ en (5.2) obtenemos

$$|h(P) - h_x(P)| \leq \frac{C''}{3},$$

que prueba (i). Obsérvese que $h(P) \geq 0$, ya que $h_x \geq 0$.

Sabemos que $\{P : h_x(P) \leq C\}$ es un conjunto finito para toda constante $C$, y también hemos visto que $h - h_x$ está acotada; entonces,

$$\#\{P : h(P) \leq C\} < \infty \qquad \forall C \in \mathbb{R}.$$

Si $P$ es un punto de torsión, entonces $\#\{[2^n]P : n \in \mathbb{N}\} < \infty$, por lo que $h(P) = 0$.

Ahora supongamos que $P$ tiene orden infinito. Como $\{Q : h(Q) < 1\}$ es un conjunto finito, debemos de tener $h([2^n]P) > 1$ para algún $n \in \mathbb{N}$. Utilizando (ii) obtenemos

$$h([2^n]P) = 4^n h(P) > 1 \Longrightarrow h(P) > \frac{1}{4^n} > 0.$$

□

**Proposición 5.1.2** *La altura canónica en $E(\mathbb{Q})$ satisface*

$$h(P \oplus Q) + h(P \ominus Q) = 2h(P) + 2h(Q).$$

*Demostración*: Si probamos que

$$h(P \oplus Q) + h(P \ominus Q) \leq 2h(P) + 2h(Q), \tag{5.3}$$

y lo aplicamos a $P' = P \oplus Q$, $Q' = P \ominus Q$ conseguiremos

$$h([2]P) + h([2]Q) \leq 2h(P \oplus Q) + 2h(P \ominus Q).$$

Dividiendo por 2 y usando la propiedad (ii) de $h$, obtenemos

$$2h(P) + 2h(Q) \leq h(P \oplus Q) + h(P \ominus Q).$$

En combinación con (5.3), esta desigualdad prueba la proposición.

Para probar (5.3) es suficiente, por la definición de $h$, probar que

$$h_x(P \oplus Q) + h_x(P \ominus Q) \leq 2h_x(P) + 2h_x(Q) + C,$$

donde $C$ es una constante independiente de $P$ y $Q$.

Si $P$ ó $Q$ es $\mathcal{O}$, la desigualdad es trivial. Si $P \oplus Q$ ó $P \ominus Q$ es $\mathcal{O}$, la desigualdad se reduce a la proposición 3.3.1. Por tanto podemos tomar

$$P = (x, y) \quad \text{con} \quad x = \frac{p}{q} \text{ y } (p, q) = 1,$$
$$Q = (x', y') \quad \text{con} \quad x' = \frac{p'}{q'} \text{ y } (p', q') = 1.$$

Denotaremos

$$x_+ = x(P \oplus Q) \quad , \quad x_- = x(P \ominus Q).$$

Como $P \neq Q$ y $P \neq \ominus Q$, la fórmula de la suma y la resta en $E(\mathbb{Q})$ nos da

$$x_\pm = \left(\frac{y' \mp y}{x' - x}\right)^2 - x - x'.$$

Utilizando que nuestra curva elíptica está dada por $y^2 = x^3 + Ax + B$ obtenemos

$$\begin{aligned} x_+ + x_- &= 2\frac{xx'(x'+x) + A(x'+x) + 2B}{(x'-x)^2} = \\ &= \frac{pp'(p'q+pq') + Aqq'(p'q+pq') + 2Bq^2q'^2}{(p'q+pq')^2}. \end{aligned} \tag{5.4}$$

y

$$\begin{aligned} x_+ \cdot x_- &= \frac{(y'^2-y^2)^2}{(x'-x)^4} - 2(x+x')\frac{(y'^2+y^2)}{(x'-x)^2} + (x+x')^2 = \\ &= \frac{(pp' - qq'A)^2 - 4qq'B(pq'+p'q)}{(p'q-pq')^2}. \end{aligned} \tag{5.5}$$

Observando (5.4) y (5.5), podemos ver que se tiene

$$x_+ + x_- = \frac{r}{t} \qquad \text{y} \qquad x_+ \cdot x_- = \frac{s}{t},$$

con

$$\max(|r|,|s|,|t|) \leq C' \cdot \max(|p|,|q|)^2 \max(|p'|,|q'|)^2, \tag{5.6}$$

donde $C'$ es independiente de $P$ y $Q$. Así, tenemos que $x_+$ y $x_-$ son las dos raíces de $X^2 - \left(\frac{r}{t}\right)X + \left(\frac{s}{t}\right) = 0$. Las raíces son $X = \frac{1}{2t}(r \pm \sqrt{r^2 - 4st})$, y así obtenemos

$$x_+ \in \frac{1}{2t}\mathbb{Z} \qquad \text{y} \qquad x_- \in \frac{1}{2t}\mathbb{Z}. \tag{5.7}$$

Escribimos

$$\begin{aligned} x_+ &= \frac{p_+}{q_+} \quad \text{con} \quad (p_+, q_+) = 1, \\ x_- &= \frac{p_-}{q_-} \quad \text{con} \quad (p_-, q_-) = 1. \end{aligned}$$

Por (5.7), $2t = \delta_+ q_+ = \delta_- q_-$ para unos ciertos enteros $\delta_+$ y $\delta_-$. Entonces

$$(\delta_+ q_+)(\delta_- q_-) = 4t^2. \tag{5.8}$$

Tenemos

$$\frac{r}{t} = x_+ + x_- = \frac{p_+}{q_+} + \frac{p_-}{q_-} = \frac{p_+q_- + p_-q_+}{q_+q_-},$$

y utilizando (5.8) obtenemos

$$(p_+q_- + p_-q_+)t = rq_+q_- = \frac{4rt^2}{\delta_+\delta_-};$$

esto es,

$$\delta_+\delta_-(p_+q_- + p_-q_+) = 4rt. \tag{5.9}$$

De

$$\frac{s}{t} = x_+ \cdot x_- = \frac{p_+p_-}{q_+q_-},$$

obtenemos

$$(p_+p_-)t = sq_+q_- = \frac{4st^2}{\delta_+\delta_-},$$

es decir,

$$(\delta_+p_+)(\delta_-p_-) = 4st. \tag{5.10}$$

Para ver que $t \mid \delta_+\delta_-$ primero fijamos un primo $p$. Por 5.10 existen enteros $a, b \geq 0$ tal que $p^a \mid \delta_+p_+$,$p^b \mid \delta_-p_-$ y $ord_pt = a+b$. Como $2t = \delta_+q_+ = \delta_-q_-$, $p^a \mid \delta_+q_+$ y $p^b \mid \delta_-q_-$, de modo que $p^a \mid mcd(\delta_+p_+, \delta_+q_+) = \delta_+$ y $p^b \mid mcd(\delta_-p_-, \delta_-q_-) = \delta_-$. Por lo tanto $p^{a+b} \mid \delta_+\delta_-$. Como $p$ era arbitrario, se tiene $t \mid \delta_+\delta_-$.

Como $t \mid \delta_+\delta_-$, entonces

$$\begin{array}{lll} \text{de (5.9)} & \text{obtenemos} & |p_+q_- + p_-q_+| \leq 4|r|, \\ \text{de (5.10)} & \text{obtenemos} & |p_+p_-| \leq 4|s|, \\ \text{de (5.8)} & \text{obtenemos} & |q_+q_-| \leq 4|t|. \end{array} \tag{5.11}$$

Ahora vamos a utilizar la siguiente desigualdad:

$$\max(|p_+|, |q_+|)\max(|p_-|, |q_-|) \leq 2\max(|p_+q_- + p_-q_+|, |p_+p_-|, |q_+q_-|).$$

Usando (5.11) y después (5.6), obtenemos

$$\begin{array}{rcl} \max(|p_+|, |q_+|)\max(|p_-|, |q_-|) & \leq & 8\max(|r|, |s|, |t|) \leq \\ & \leq & 8C'\max(|p|, |q|)^2\max(|p'|, |q'|)^2, \end{array}$$

es decir,

$$H(P \oplus Q)H(P \ominus Q) \leq 8C'H(P)^2H(Q)^2;$$

y tomando logaritmos

$$h_x(P \oplus Q) + h_x(P \ominus Q) \leq C + 2h_x(P) + 2h_x(Q),$$

donde $C = log(8C')$ no depende ni de $P$ ni de $Q$. Por tanto, si tomamos límites tenemos demostrada la desigualdad (5.3) y por tanto la proposición.

□

## 5.2 Forma bilineal de Nerón-Tate.

Vamos a definir una forma bilineal asociada a la altura canónica.

**Proposición 5.2.1** *Sea $E$ una curva elíptica definida por*

$$E : y^2 = x^3 + Ax + B, \qquad \text{con } A, B \in \mathbb{Z}.$$

*Existe una única forma $\mathbb{Z}$-bilineal $\langle P, Q\rangle$ en $E(\mathbb{Q})$ tal que $\langle P, P\rangle = h(P)$. A $\langle , \rangle$ se denomina* **forma bilineal de Nerón-Tate**. *Además, esta forma desciende a $E(\mathbb{Q})/E(\mathbb{Q})_{tors} \cong \mathbb{Z}^r$ y es definida positiva ahí.*

Antes de la demostración veamos un resultado que nos será útil.

**Teorema de Minkowski.** *Sea $F$ un subconjunto de $\mathbb{R}^r$ conteniendo al $0$, compacto, convexo y simétrico con respecto a $0$. Si el volumen de $F$ ,$vol(F)$, es mayor que $4^r$, entonces $F$ contiene un elemento de $\mathbb{Z}^r$ distinto del $0$.*

*Demostración*: Sea $N$ un entero suficientemente grande tal que el cubo $C$ con centro en 0 y arista de longitud $4N$ contiene a $F$. Supongamos que $(F \setminus \{0\}) \cap \mathbb{Z}^r$ es vacía. Veamos que $\{x + \frac{1}{2}F\}_{x\in\mathbb{Z}^r}$ son disjuntos. Si no lo fueran, tendríamos

$$x_1 + \frac{1}{2}f_1 = x_2 + \frac{1}{2}f_2$$

con $x_1 \neq x_2$. Entonces $x_1 - x_2 = \frac{1}{2}(f_1 - f_2)$, y esto pertenecería a $F$ por ser $F$ simétrico y convexo, y a $\mathbb{Z}^r \setminus \{0\}$, lo que contradice $(F \setminus \{0\}) \cap \mathbb{Z}^r = \emptyset$.

Considero $x \in \mathbb{Z}^r$ tal que $|x|_\infty := \max\{|x_1|, \ldots, |x_r|\} \leq N$, entonces $x + \frac{1}{2}F \subset C$. Por tanto,

$$\begin{aligned} vol(C) = (4N)^r &\geq \sum_{\substack{x \in \mathbb{Z}^r \\ tal que |x|_\infty \leq N}} vol\left(x + \frac{1}{2}F\right) \\ &\geq (2N)^r vol\left(\frac{1}{2}F\right) = 2^{-r}(2N)^r vol(F). \end{aligned}$$

Como $vol(F) > 4^r$ por hipótesis, esto es una contradicción.

□

*Demostración de la proposición 5.2.1*: Como la forma ha de ser bilineal, ha de cumplirse

$$\langle P \oplus Q, P \oplus Q\rangle = \langle P, P\rangle - 2\langle P, Q\rangle + \langle Q, Q\rangle.$$

Como se ha de cumplir que $h(P) = \langle P, P\rangle$, si la forma bilineal existe ha de estar dada por

$$\boxed{\langle P, Q\rangle = \tfrac{1}{2}\left[h(P \oplus Q) - h(P) - h(Q)\right]}.$$

Esto nos da la unicidad y la simetría de la forma bilineal.

Para la linealidad en la primera variable, vamos a usar la proposición 5.1.2 repetidas veces. Primero tenemos:

$$\begin{array}{rcl}\langle \ominus P, Q\rangle = & \frac{1}{2}\left[h(Q\ominus P) - h(P) - h(Q)\right] = \\ = & -\frac{1}{2}\left[h(P\oplus Q) - h(P) - h(Q)\right] = & -\langle P, Q\rangle.\end{array} \tag{5.12}$$

Entonces podemos escribir

$$\begin{array}{l}\langle P\oplus P', Q\rangle + \langle P\ominus P', Q\rangle = \\ = \frac{1}{2}\left[h(P\oplus P'\oplus Q) + h(P\ominus P'\oplus Q)\right. \\ \left. -h(P\oplus P') - h(P\ominus P') - h(P) - h(Q)\right] = \\ = \frac{1}{2}\left[2h(P\oplus Q) + 2h(P') - 2h(P) - 2h(P') - 2h(Q)\right] = \\ = 2\langle P, Q\rangle.\end{array} \tag{5.13}$$

Intercambiando $P$ y $P'$ y usando (5.12), obtenemos

$$\langle P\oplus P', Q\rangle - \langle P\ominus P', Q\rangle = 2\langle P', Q\rangle,$$

sumando esto a (5.13) tenemos

$$\langle P\oplus P', Q\rangle = \langle P, Q\rangle + \langle P', Q\rangle.$$

Por último utilizando la simetría de la forma $\langle , \rangle$, obtenemos la bilinealidad.

Observamos que para todos $m, n \in \mathbb{Z}$ y para todo $P, Q \in E(\mathbb{Q})$ se tiene

$$-2mn\langle P, Q\rangle = 2\langle \ominus[m]P, [n]Q\rangle = h([n]Q\ominus[m]P) - h([m]P) - h([n]Q),$$

y entonces,

$$0 \le h([n]Q\ominus[m]P) = m^2h(P) - 2\langle \ominus[m]P, [n]Q\rangle + n^2h(Q);$$

es decir, el polinomio

$$x^2h(P) - 2x\langle P, Q\rangle + h(Q)$$

es $\ge 0$ para todo $x \in \mathbb{Q}$, y por consiguiente para todo $x \in \mathbb{R}$. Entonces,

$$4\langle P, Q\rangle^2 - 4h(P)h(Q) \le 0 \Longrightarrow \boxed{|\langle P, Q\rangle|^2 \le h(P)h(Q)}.$$

A esta desigualdad se le conoce con el nombre de **desigualdad de Schwartz**.

Ahora, si $Q \in E(\mathbb{Q})_{tors}$, tenemos que $h(Q) = 0$ y usando la desigualdad de Schwartz obtenemos

$$\langle P, Q\rangle = 0 \quad \forall P \in E(\mathbb{Q}).$$

Por tanto $Q \in E(\mathbb{Q})^{\perp}$ con respecto a $\langle , \rangle$. Luego

$$0 = \langle P, Q\rangle = \frac{1}{2}(h(P\oplus Q) - h(P) - h(Q)) \Longrightarrow h(P\oplus Q) = h(P).$$

Esto es,

$$\langle P\oplus Q, P'\oplus Q'\rangle = \langle P, P'\rangle \quad \forall P, P' \in E(\mathbb{Q}),\ \forall Q, Q' \in E(\mathbb{Q})_{tors}.$$

Por tanto, $\langle , \rangle$ desciende a $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$. Y además:

**Observación 5.2.2** $\langle , \rangle = 0 \Longleftrightarrow E(\mathbb{Q}) = E(\mathbb{Q})_{tors}$.

Si $\{P_1, \ldots, P_r\}$ es una base de $E(\mathbb{Q})/E(\mathbb{Q})_{tors} \cong \mathbb{Z}^r$, entonces $\langle , \rangle$ está determinada por la matriz $(c_{ij})$, donde $c_{ij} := \langle P_i, P_j \rangle$.

Así, tenemos

$$0 \leq h\left(\sum_{i=1}^{r} m_i P_i\right) = \langle \sum_{i=1}^{r} m_i P_i, \sum_{i=1}^{r} m_i P_i \rangle = \sum_{i,j=1} m_i c_{ij} m_j.$$

Si ponemos $\lambda_i = \frac{m_i}{N}$ y $\lambda_j = \frac{m_j}{N}$ obtenemos:

$$\sum_{i,j=1}^{r} \lambda_i c_{ij} \lambda_j \geq 0 \qquad \forall \lambda_i, \lambda_j \in \mathbb{Q}.$$

Entonces $\langle , \rangle$ es semidefinida positiva en $E(\mathbb{Q})$. De hecho, pasando al límite vemos que

$$\sum_{i,j=1}^{r} \lambda_i c_{ij} \lambda_j \geq 0 \quad \forall \lambda_i, \lambda_j \in \mathbb{R},$$

es decir, $\langle , \rangle$ es semidefinida positiva en $E(\mathbb{Q}) \otimes \mathbb{R}$.

Veamos, por último, que es definida positiva. Como $(c_{ij})$ es simétrica y semidefinida positiva, podemos elegir los vectores columna $v_1, \ldots, v_r$ que forman una base de autovectores de $(c_{ij})$ con autovalores respectivamente $\lambda_1 \geq \ldots \geq \lambda_r \geq 0$. Vamos a probar que $\lambda_r > 0$. Supongamos

$$\lambda_r = 0.$$

Sea $\{e_1, \ldots, e_r\}$ la base ortonormal usual de $\mathbb{R}^r$; podremos escribir

$$v_k = \sum_{i=1}^{r} v_{ki} e_i.$$

Identificamos $P = \sum_{i=1}^{r} m_i P_i$ con el vector columna $\sum_{i=1}^{r} m_i e_i$. Así la forma $\langle , \rangle$ está dada por

$$\langle \sum_{i=1}^{r} a_i e_i, \sum_{j=1}^{r} a'_j e_j \rangle = \sum_{i,j=1}^{r} a_i c_{ij} a'_j.$$

Entonces,

$$\begin{aligned} \langle \sum_{k=1}^{r} b_k v_k, \sum_{l=1}^{r} b_l v_l \rangle &= \langle \sum_{k,i=1}^{r} b_k v_{ki} e_i, \sum_{l,j=1}^{r} b_l v_{lj} e_j \rangle = \\ &= \sum_{k,l=1}^{r} b_k b_l \sum_{i,j=1}^{r} v_{ki} c_{ij} v_{lj} = \end{aligned}$$

$$= \sum_{k,l=1}^{r} b_k b_l \sum_{i=1}^{r} \lambda_l v_{ki} v_{li} =$$
$$= \sum_{k=1}^{r} \lambda_k b_k^2,$$

ya que los vectores $v_k$ son ortonormales.

Sea $\epsilon = \min\{h(P) = \langle P, P\rangle : P \notin E(\mathbb{Q})_{tors}\}$. Como $\{P : h(P) \leq C\}$ es un conjunto finito para toda constante $C$, se tiene que $\epsilon$ existe. Y como $h(P) > 0$ para todo $P \notin E(\mathbb{Q})_{tors}$ se tiene que $\epsilon > 0$. Sea $F$ el conjunto compacto, convexo y simétrico siguiente:

$$F := \left\{ \sum_{i=1}^{r} b_k v_k : \max_{1\leq k\leq r-1} |b_k| \leq \left(\frac{\epsilon}{2r\lambda_1}\right)^{1/2} \text{ y } |b_r| \leq M \right\},$$

con $M$ elegido suficientemente grande para que $vol(F) > 4^r$. Por el Teorema de Minkowski, $F$ contiene un elemento no nulo $P = \sum_{i=1}^{r} b_i v_i \in E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ con $b_i \in \mathbb{Z}$. Pero entonces

$$\begin{aligned} h(P) &= \langle \sum_{i=1}^{r} b_i v_i, \sum_{j=1}^{r} b_j v_j \rangle = \sum_{i=1}^{r} \lambda_i b_i^2 \\ &= \sum_{i=1}^{r-1} \lambda_i b_i^2 \leq \sum_{i=1}^{r-1} \lambda_1 \left(\frac{\epsilon}{2r\lambda_1}\right) < \frac{\epsilon}{2}, \end{aligned}$$

ya que hemos supuesto que $\lambda_r = 0$ y que $P \in F$. Sim embargo esto representa una contradicción debido a que hemos encontrado un elemento $P \in E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ tal que $h(P) \leq \frac{\epsilon}{2}$. Esto prueba que $(c_{ij})$ es definida positiva y concluye la demostración de la proposición.

□

## 5.3 Fórmula geométrica del rango.

En esta sección vamos a dar una fórmula para obtener el rango. Para ello la herramienta principal es la forma bilineal de Nerón-Tate, definida en la sección anterior.

La matriz $(\langle P_i, P_j\rangle)_{1\leq i,j\leq r}$ depende de la elección de la base $\{P_1, \ldots, P_r\}$ de $\mathbb{Z}^r$, pero el determinante no. De ahí la siguiente definición.

**Definición.** *Se define el* **regulador elíptico de** $E$ *sobre* $\mathbb{Q}$ *como el número*

$$R_{E/\mathbb{Q}} := det(\langle P_i, P_j\rangle).$$

**Proposición 5.3.1** *Sea $E$ una curva elíptica dada por*

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Z}.$$

*Entonces*

$$\lim_{t\to\infty} \#\{(x,y) \in E(\mathbb{Q}) : h(P) \le t\} \begin{cases} = \#E(\mathbb{Q})_{tors} & si\ r = 0, \\ \sim \dfrac{\Omega_r \#E(\mathbb{Q})_{tors}}{R_E^{1/2}}\, t^{r/2} & si\ r > 0, \end{cases}$$

*donde $\Omega_r$ es el volumen de la bola unidad en $\mathbb{R}^r$ y $R_E$ es el regulador elíptico de $E/\mathbb{Q}$.*

*Demostración*: Si $r = 0$ es obvio. Supongamos que $r > 0$. Tenemos la matriz definida positiva $(c_{ij}) := \langle P_i, P_j \rangle$. Tomando $e_i$ la base usual de $\mathbb{R}^r$ y usando el siguiente resultado de Análisis de Fourier euclídeo:

$$\lim_{t\to\infty} \# \left\{ \sum_{i=1}^{r} n_i e_i : n_i \in \mathbb{Z} \text{ y } \sum_{i=1,j}^{r} n_i c_{ij} n_j \le t \right\} \sim \frac{\Omega_r t^{r/2}}{[det(c_{ij})]^{1/2}},$$

se tiene que

$$\lim_{t\to\infty} \# \left\{ \begin{array}{l} \displaystyle\sum_{i=1}^{r} [n_i]P_i \oplus Q : n_i \in \mathbb{Z},\ Q \in E(\mathbb{Q})_{tors} \\ \qquad \text{y tal que } h\left( \displaystyle\sum_{i=1}^{r} [n_i]P_i \oplus Q \right) \le t \end{array} \right\} \sim \frac{\Omega_r \#E(\mathbb{Q})_{tors}}{R_{E/\mathbb{Q}}^{1/2}}\, t^{r/2}.$$

□

## 5.4 Cota superior para el rango.

Aunque la proposición 5.3.1 nos da una fórma de hallar el rango de $E(\mathbb{Q})$, la fórmula no es muy práctica como herramienta de cálculo. En esta sección daremos una aproximación diferente para estimar el rango, utilizaremos la cota del orden de $E(\mathbb{Q})/2E(\mathbb{Q})$.

Recordamos que existe un dominio $R$ para el que teníamos (ver proposición 3.2.7):

$$E(K)/2E(K) \hookrightarrow \left(\{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \{\mathcal{U}(R)/\mathcal{U}^2(R)\}\right) \oplus \bigoplus_{\substack{p \text{ primo en } R \\ \text{tal que } p \,|\, d}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}).$$

Por tanto,

$$\#\, E(K)/2E(K) \le \#\, \left(\{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \{\mathcal{U}(R)/\mathcal{U}^2(R)\}\right) \oplus \bigoplus_{\substack{p \text{ primo en } R \\ \text{tal que } p \,|\, d}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}).$$

Por consiguiente,

$$\boxed{\#\, E(K)/2E(K) \leq [\#\ \{\mathcal{U}(R)/\mathcal{U}^2(R)\}]^2 \cdot 2^{2\,\#\{p \text{ primo en } R\colon\ p \mid d\}}.} \tag{5.14}$$

Además, utilizando la proposición 3.2.1 obtenemos

$$\#\, E(\mathbb{Q})/2E(\mathbb{Q}) \leq \#\, E(K)/2E(K)\ +\ 4^{[K:\mathbb{Q}]}. \tag{5.15}$$

Vamos a diferenciar varios casos, dependiendo del número de puntos de 2-torsión que tenga $E(\mathbb{Q})$. Si tenemos una curva elíptica dada por

$$E : y^2 = x^3 + Ax + B = (x-\alpha)(x-\beta)(x-\gamma),$$

los puntos de 2-torsión en $E(\mathbb{C})$ corresponden a los puntos $(\alpha, 0), (\beta, 0)$ y $(\gamma, 0)$. Por lo tanto si nos preguntamos por los puntos de 2-torsión en $E(\mathbb{Q})$ sólo hay tres posibilidades:

- $\alpha, \beta, \gamma \notin \mathbb{Z}$. Entonces $E(\mathbb{Q})_{tors}$ no tiene como subgrupo a $\mathbb{Z}/2\mathbb{Z}$ y por el Teorema de Mazur obtenemos

  $$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/(2N+1)\mathbb{Z} \qquad 1 \leq 2N+1 \leq 9.$$

  Por tanto,

  $$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r\,.$$

  Utilizando (5.14) y (5.15) tenemos:

  $$\#\, E(\mathbb{Q})/2E(\mathbb{Q}) = 2^r \leq \left[\#\ \left\{\mathcal{U}(R)/\mathcal{U}^2(R)\right\}\right]^2 \cdot 2^{2\,\#\{p \text{ primo en } R\ :\ p \mid d\}} + 4^{[K:\mathbb{Q}]},$$

  y entonces,

  $$\boxed{r \leq log_2 \left[[\#\ \{\mathcal{U}(R)/\mathcal{U}^2(R)\}]^2 \cdot 2^{2\,\#\{p \text{ primo en } R\ :\ p \mid d\}} + 4^{[K:\mathbb{Q}]}\right]}$$

- $\alpha \in \mathbb{Z}; \beta, \gamma \notin \mathbb{Z}$. Entonces $E(\mathbb{Q})_{tors}$ contiene a $\mathbb{Z}/2\mathbb{Z}$, pero no a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. El Teorema de Mazur nos dice entonces que

  $$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2N\mathbb{Z} \qquad 1 \leq 2N \leq 12.$$

  Por tanto,

  $$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^r\,.$$

  Utilizando de nuevo (5.14) y (5.15) tenemos que

  $$\#\, E(\mathbb{Q})/2E(\mathbb{Q}) = 2^{r+1} \leq \left[\#\ \left\{\mathcal{U}(R)/\mathcal{U}^2(R)\right\}\right]^2 \cdot 2^{2\,\#\{p \text{ primo en } R\ :\ p \mid d\}} + 4^{[K:\mathbb{Q}]},$$

  y entonces,

  $$\boxed{r \leq log_2 \left[[\#\ \{\mathcal{U}(R)/\mathcal{U}^2(R)\}]^2 \cdot 2^{2\,\#\{p \text{ primo en } R\ :\ p \mid d\}} + 4^{[K:\mathbb{Q}]}\right] - 1} \tag{5.16}$$

- $\alpha, \beta, \gamma \in \mathbb{Z}$. Entonces $E[2](\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, y el Teorema de Mazur nos dice que
$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} \qquad 1 \leq N \leq 4,$$
por lo que
$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^r .$$
Utilizando la observación 3.2.8 tenemos que
$$\# E(\mathbb{Q})/2E(\mathbb{Q}) = 2^{r+2} \leq 2^2 \cdot 2^{2\,\#\{p \text{ primo en } R \,:\, p \,|\, d\}},$$
y que
$$\boxed{r \leq 2\,\#\{p \text{ primo en } \mathbb{Z}\colon\ p \,|\, d\}} \tag{5.17}$$

A partir de ahora vamos a considerar sólo el caso en que tenemos una curva elíptica definida por
$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) \qquad \alpha, \beta, \gamma \in \mathbb{Z}.$$
En estas[1] condiciones vamos a poder encontrar una cota mucho mejor que la cota 5.17 para el rango de $E(\mathbb{Q})$. Además vamos a ver que cuanto peor es la reducción en cada primo $p$, más nos va a contribuir a que la curva tenga rango alto.

**Definición.** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$ y dada por*
$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) \qquad \alpha, \beta, \gamma \in \mathbb{Z}.$$
*Sea $p$ un primo en $\mathbb{Z}$. Consideramos la reducción módulo $p$ definida en la sección §4.1.1. Diremos que:*
$$p \text{ es} \begin{cases} \textbf{de buena reducción} \\ \textbf{de (mala) reducción multiplicativa} \\ \textbf{de (mala) reducción aditiva} \end{cases} \iff$$
$$\iff \begin{cases} p \not| \Delta = (\alpha-\beta)(\alpha-\gamma)(\beta-\gamma), \\ p \,|\ \textit{a sólo uno de los factores } (\alpha-\beta), (\alpha-\gamma), (\beta-\gamma), \\ p \,|\, (\alpha-\beta), (\alpha-\gamma), (\beta-\gamma). \end{cases}$$

Denotaremos:
$$\begin{aligned} n_1 &:= \#\{p \text{ primo} : p \text{ es de mala reducción multiplicativa}\}, \\ n_2 &:= \#\{p \text{ primo} : p \text{ es de mala reducción aditiva}\}. \end{aligned}$$

**Teorema 5.4.1** *Con las hipótesis anteriores tenemos que*
$$\boxed{r \leq n_1 + 2n_2 - 1}$$

[1] También se puede encontrar una cota mejor para el caso en que no ocurre que $\alpha, \beta, \gamma \in \mathbb{Z}$, pero tiende a ser muy grande.

*Demostración*: Por la observación 3.2.8,

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \bigoplus_{\pm, p \mid d} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}).$$

Vamos a ver que la imagen en la coordenada $\pm$ cae en un subgrupo $\mathbb{Z}/2\mathbb{Z}$ de $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ y lo mismo es cierto para la $p$-ésima coodenada si $p$ es de reducción multiplicativa. Así obtenemos

$$2^{1+n_1+2n_2} \geq 2^{r+2} = \# E(\mathbb{Q})/2E(\mathbb{Q}).$$

Primero consideramos la coordenada $\pm$. Las raíces $\alpha, \beta, \gamma$ son enteros y pueden ser ordenados. Supongamos $\alpha < \beta < \gamma$, por lo que

$$x - \alpha > x - \beta > x - \gamma. \tag{5.18}$$

Si $x \notin \{\alpha, \beta, \gamma\}$, los posibles signos en (5.18) son *a priori*:

$$+++ \quad , \quad ++- \quad , \quad +-- \quad , \quad ---,$$

pero tenemos $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$; por tanto las únicas posibilidades son

$$+++ \quad y \quad +--\,.$$

Entonces usando la definición de $\varphi_\alpha$ dada en la sección 3.2 tenemos que si $P = (x, y)$, $\varphi_\alpha(P) = x - \alpha > 0$, por lo que la coordenada $\pm$ de $\varphi_\alpha \times \varphi_\beta(P)$ cae en $0 \oplus \mathbb{Z}/2\mathbb{Z}$. (Si en vez de tomar $\varphi_\alpha \times \varphi_\beta$ usamos $\varphi_\alpha \times \varphi_\gamma$ ó $\varphi_\beta \times \varphi_\gamma$, entonces la imagen en la coordenada $\pm$ cae en $0 \oplus \mathbb{Z}/2\mathbb{Z}$ y en $diag(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) = \{(0,0),(1,1)\}$ respectivamente).

Y si $x \in \{\alpha, \beta, \gamma\}$ obtenemos:

- $x = \alpha$, entonces $\varphi_\alpha(P) = (\beta - \alpha)(\gamma - \alpha) > 0$.
- $x = \beta$, entonces $\varphi_\alpha(P) = (\beta - \alpha) > 0$.
- $x = \gamma$, entonces $\varphi_\alpha(P) = (\gamma - \alpha) > 0$.

Ahora sea $p$ un primo de mala reducción multiplicativa, digamos que $p \,|\, \alpha - \beta$. Sea $P = (x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathcal{O}\}$. Y supongamos que $x \notin \{\alpha, \beta, \gamma\}$. Definimos los enteros $a, b, c$ como

$$a = ord_p(x - \alpha) \quad , \quad b = ord_p(x - \beta) \quad y \quad c = ord_p(x - \gamma).$$

Denotaremos a la coordenada $p$-ésima por:

$$\pi_p(\varphi_\alpha \times \varphi_\beta(P)) := (a \bmod 2, b \bmod 2).$$

Como $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$,

$$a + b + c \equiv 0 \bmod 2.$$

Además vimos que si alguno de $a, b, c$ es menor que 0, entonces

$$a \equiv b \equiv c \equiv 0 \bmod 2,$$

esto es,

$$\pi_p(\varphi_\alpha \times \varphi_\beta(P)) = (0,0).$$

Si $a, b, c = 0$, deducimos que $\pi_p(\varphi_\alpha \times \varphi_\beta(P)) = (0,0)$.

Si $a > 0$, entonces $p \,|\, (x-\alpha)$. Como $x - \gamma = (x-\alpha) + (\alpha - \gamma)$ y $p \not| (\alpha - \gamma)$, entonces,

$$c = ord_p(x-\gamma) = ord_p((x-\alpha) + (\alpha - \gamma)) = 0,$$

y por lo tanto, $a + b \equiv 0 \bmod 2$, es decir:

$$\pi_p(\varphi_\alpha \times \varphi_\beta(P)) = \begin{cases} (0,0) \\ \text{ó} \\ (1,1) \end{cases}.$$

Por tanto

$$\pi_p(\varphi_\alpha \times \varphi_\beta(P)) \in diag(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}).$$

Si $b > 0$ igual.

Si $c > 0$, entonces $p \,|\, (x-\gamma)$. Como

$$\begin{gathered} x - \alpha = (x-\gamma) + (\gamma - \alpha) \ , \ p \not| (\gamma - \alpha) \\ y \\ x - \beta = (x-\gamma) + (\gamma - \beta) \ , \ p \not| (\gamma - \beta) \end{gathered}$$

entonces,

$$\begin{gathered} a = ord_p(x-\alpha) = ord_p((x-\gamma) + (\gamma - \alpha)) = 0 \\ y \\ b = ord_p(x-\beta) = ord_p((x-\gamma) + (\gamma - \beta)) = 0. \end{gathered}$$

Por tanto,

$$\pi_p(\varphi_\alpha \times \varphi_\beta(P)) = (0,0).$$

Ahora supongamos $x \in \{\alpha, \beta, \gamma\}$. Entonces,

- Si $x = \alpha$, entonces $\varphi_\alpha(\alpha, 0) = (\beta - \alpha)(\gamma - \alpha)$ y $\varphi_\beta(\alpha, 0) = (\beta - \alpha)$; como

$$\frac{\varphi_\alpha(\alpha,0)}{\varphi_\beta(\alpha,0)} = (\gamma - \alpha)$$

no es divisible por $p$, entonces

$$\pi_p(\varphi_\alpha \times \varphi_\beta(\alpha, 0)) \in diag(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}).$$

- Si $x = \beta$, entonces $\varphi_\alpha(\beta, 0) = (\beta - \alpha)$ y $\varphi_\beta(\beta, 0) = (\alpha - \beta)(\gamma - \beta)$; como

$$\frac{\varphi_\alpha(\beta, 0)}{\varphi_\beta(\beta, 0)} = (\beta - \gamma)$$

  no es divisible por $p$, entonces

$$\pi_p(\varphi_\alpha \times \varphi_\beta(\beta, 0)) \in diag(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}).$$

- Si $x = \gamma$, entonces $\varphi_\alpha(\gamma, 0) = (\gamma - \alpha)$ y $\varphi_\beta(\gamma, 0) = (\gamma - \beta)$; como no son divisibles por $p$, entonces

$$\pi_p(\varphi_\alpha \times \varphi_\beta(\gamma, 0)) = (0, 0).$$

Conclusión,

$$\pi_p(\varphi_\alpha \times \varphi_\beta(E(\mathbb{Q})/2E(\mathbb{Q}))) \subset diag(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}).$$

Análogamente,

$$\text{si } p \,|\, (\beta - \gamma) \implies \pi_p(\varphi_\alpha \times \varphi_\beta(E(\mathbb{Q})/2E(\mathbb{Q}))) \subset 0 \oplus \mathbb{Z}/2\mathbb{Z},$$

$$\text{si } p \,|\, (\alpha - \gamma) \implies \pi_p(\varphi_\alpha \times \varphi_\beta(E(\mathbb{Q})/2E(\mathbb{Q}))) \subset \mathbb{Z}/2\mathbb{Z} \oplus 0.$$

□

# Capítulo 6

# Algunas conjeturas de la Teoría de Curvas elípticas.

Este capítulo está dedicado a enunciar algunas de las conjeturas más importantes en la teoría de curvas elípticas.

En primer lugar definiremos la función zeta de una variedad algebraica proyectiva. Enunciaremos el Teorema de Weil-Deligne, que nos será necesario para poder definir la función $L$ asociada a una curva elíptica. También nos será útil en el capítulo siguiente.

En la sección §6.3 enunciaremos la conjetura de Shimura-Taniyama-Weil, una de las conjeturas más importantes en la actualidad y en la que Taylor y Wiles han hecho grandes progresos en los últimos años. Otra de las conjeturas fundamentales en la teoría de curvas elípticas fue formulada por Birch y Swinnerton-Dyer después de hacer una gran cantidad de cálculos computacionales. Esta conjetura establece que el rango de una curva elíptica es igual al orden del cero de su función $L$ asociada en el punto 1. La sección §6.4 está dedicada a enunciar los últimos resultados obtenidos en torno a esta conjetura.

Y por último, enunciaremos la conjetura que establece que existen curvas elípticas definidas sobre $\mathbb{Q}$ de rango arbitrariamente alto. De momento se sabe que existen curvas elípticas de rango al menos 22. El próximo capítulo está dedicado a ver algunos ejemplos de curvas elípticas de rango alto.

En definitiva, este capítulo está dedicado a intentar dar una visión del estado de estas conjeturas en la actualidad.

## 6.1 La función Zeta de una variedad algebraica.

En 1949 A. Weil hizo algunas conjeturas muy generales en torno al número de puntos de una variedad definida sobre un cuerpo finito. En esta sección vamos a enunciar la conjetura de Weil.

Sea $\mathbb{F}_q$ un cuerpo con $q$ elementos, y para cada $n \geq 1$ consideramos $\mathbb{F}_{q^n}$ una extensión de $\mathbb{F}_q$ de grado $n$. Sea $V$ una variedad proyectiva definida sobre $\mathbb{F}_q$ y sea $V(\mathbb{F}_{q^n})$ el conjunto de puntos de $V$ sobre $\mathbb{F}_{q^n}$. Ahora consideramos la siguiente serie formal de potencias en la variable $T$:

$$Z_q(T) := exp\left(\sum_{n\geq 1} \frac{|V(\mathbb{F}_{q^n})|}{n} T^n\right).$$

Entonces tenemos el siguiente Teorema, primero conjeturado por Weil y probado por él para curvas y variedades abelianas ([WE3]) y demostrado completamente por Deligne ([DEL]) en 1974.

**Teorema de Weil-Deligne.** *Sea $V$ una variedad proyectiva lisa de dimensión $d$ sobre $\mathbb{F}_q$. Entonces,*

*(i) La serie $Z_q(T)$ es una función racional en $T$, es decir,*

$$Z_q(T) \in \mathbb{Q}(T).$$

*(ii) Existe un entero $e$, llamado la* **caracteristica de Euler de** *$V$, tal que*

$$Z_q\left(\frac{1}{q^d T}\right) = \pm q^{de/2} T^e\, Z_q(T).$$

*(iii) La función racional $Z_q(T)$ factoriza como sigue:*

$$Z_q(T) = \frac{P_1(T)\cdots P_{2d-1}(T)}{P_0(T)\cdots P_{2d}(T)},$$

*donde para todo $i$, $P_i(T) \in \mathbb{Z}[T]$. Además $P_0(T) = 1 - T, P_{2d}(T) = 1 - q^d T$ y para $i = 1, \ldots, 2d-1$:*

$$P_i(T) = \prod_j (1 - \alpha_{ij} T)$$

*con $\alpha_{ij} \in \mathbb{C}$ tales que $|\alpha_{ij}| = q^{i/2}$.*

La primera afirmación fue probada algunos años antes que Deligne, en 1960 por B. Dwork([DWO]). La parte con mayor dificultad es la prueba de la última afirmación, que $|\alpha_{ij}| = p^{i/2}$. Esta es la llamada *hipótesis de Riemann para variedades sobre cuerpos finitos.*

Ahora, dadas todas las funciones $Z_p(T)$, con $p$ primo, podemos formar una función zeta global, definida para complejos $s$ con $Re(s)$ suficientemente grande:

$$\zeta_V(s) := \prod_p Z_p(p^{-s}).$$

Muy poco se sabe sobre esta función. Se conjetura que posee una continuación analítica a todo el plano complejo como una función meromorfa con una ecuación funcional cuando los factores locales en los primos malos $p$ son elegidos correctamente, y que satisface la hipótesis de Riemann, es decir que aparte de los ceros y polos "triviales", el resto de ceros y polos están en cierta recta vertical en el plano complejo.

## 6.2 Funciones $L$ de curvas elípticas.

Ahora consideramos el caso especial en el que $V$ es una curva elíptica $E$. Enunciamos el siguiente teorema, que es simplemente el caso especial de la conjetura de Weil para curvas elípticas (para una demostración, ver [SIL], páginas 134-136).

**Teorema de Hasse.** *Sea $E$ una curva elíptica definida sobre $\mathbb{F}_q$. Entonces existe un número algebraico $\alpha_q$, tal que*

*(i)* $|E(\mathbb{F}_{q^n})| = q^n + 1 - \alpha_q^n - \overline{\alpha}_q^n$.

*(ii)* $|\alpha_q| = \sqrt{q}$.

El teorema de Hasse nos da toda la información necesaria sobre el número de puntos de $E$ sobre un cuerpo finito. Y obtenemos el siguiente corolario:

**Corolario.** *Sea $E$ una curva elíptica definida sobre $\mathbb{F}_q$. Entonces existe un $a_q \in \mathbb{Z}$ tal que*

$$Z_q(T) = \frac{1 - a_q T + qT^2}{(1-T)(1-qT)},$$

*donde* $a_q = q + 1 - |E(\mathbb{F}_q)|$.

Este resultado es una simple aplicación del apartado (iii) del teorema de Weil-Deligne al caso $d = 1$.

Ignorando de momento el caso de primos de mala reducción, la definición general de función zeta nos da

$$\zeta_E(s) = \frac{\zeta(s)\zeta(s-1)}{L_E(s)},$$

donde

$$L_E(s) := \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

y $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ es la función zeta de Riemann. La función $L_E(s)$ se llama función $L$ de Hasse-Weil de la curva elíptica $E$. Para definirla de forma más precisa necesitamos por un lado definir los factores locales en los primos de mala reducción, y por otro necesitamos que la ecuación de nuestra curva elíptica sea un tanto especial para que la función $L$ este bien definida. Para ello vamos a definir lo que es una ecuación minimal de Weierstrass.

**Definición.** *Sea $E$ una curva elíptica definida por una ecuación de Weierstrass con coeficientes en $\mathbb{Z}$. El discriminante $\Delta$ será entonces un entero, y la norma p-ádica satisface $|\Delta|_p \leq 1$, con igualdad si y sólo si $p \not| \Delta$. Una ecuación de Weierstrass se dice que es* **minimal en el primo** *$p$ si $|\Delta|_p$ no puede crecer reemplazando $(x, y)$ por $(u^{-2}x, u^{-3}y)$ para $u \in \mathbb{Z}$ de forma que los nuevos coeficientes son enteros p-ádicos. Se dice que una ecuación de Weierstrass para $E$ es* **globalmente minimal** *si es minimal para todo primo y si sus coeficientes son enteros.*

El resultado siguiente, debido a Nerón, nos asegura que toda curva elíptica definida sobre $\mathbb{Q}$ tiene una ecuación globalmente minimal.

**Teorema 6.2.1** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$, entonces existe un cambio de variables sobre $\mathbb{Q}$ tal que la ecuación resultante es una ecuación de Weierstrass globalmente minimal.*

*Demostración:* Ver [KNA], Teorema 10.3.

**Definición.** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$ y sea*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

*una ecuación de Weierstrass globalmente minimal para $E$. Sea $p$ un primo, entonces:*

- *Si $E$ tiene buena reducción en $p$, definimos*

$$a_p := p + 1 - |E_p(\mathbb{F}_p)|.$$

- *Si $E$ tiene mala reducción en $p$, es decir si $p \,|\, \Delta$, definimos*

$$\epsilon(p) := \begin{cases} 1 & \text{si } E \text{ tiene reducción multiplicativa split en } p, \\ -1 & \text{si } E \text{ tiene reducción multiplicativa no split en } p, \\ 0 & \text{si } E \text{ tiene reducción aditiva en } p. \end{cases}$$

*Entonces definimos la* **función L de Hasse-Weil de** *$E$, para $Re(s) > \frac{3}{2}$, como*

$$L_E(s) := \prod_{p \,|\, \Delta} (1 - \epsilon(p)p^{-s})^{-1} \prod_{p \not| \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

**Observación 6.2.2** En esta definición es crucial tomar una ecuación de Weierstrass globalmente minimal para $E$, ya que tomando otra ecuación podría crecer el número de primos de mala reducción, y entonces cambiar un número finito de factores locales.

Vamos a enunciar la primera de las conjeturas sobre funciones $L$ de curvas elípticas.

**Conjetura 1.** *La función $L_E(s)$ puede ser continuada analíticamente a todo el plano complejo como una función meromorfa. Además, existe un entero positivo $N$ tal que si definimos*

$$\Lambda_E(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s),$$

*tenemos la siguiente ecuación funcional,*

$$\Lambda_E(2-s) = \pm\Lambda_E(s).$$

En este caso, la hipótesis de Riemann establece que aparte de ceros triviales en enteros negativos, los ceros de $L_E(s)$ están todos en la línea crítica $Re(s) = 1$. Weil probó esta conjetura para dos casos especiales. En 1954, Deuring la demostró cuando $E$ tiene multiplicación compleja, es decir, cuando $End(E)$ es un anillo estrictamente mayor que $\mathbb{Z}$. Eichler (1954) y Shimura (1958) la probaron cuando $E$ es una curva elíptica modular[1]. En cualquier caso, si $E$ tiene multiplicación compleja, o más en general, si $E$ es una curva elíptica modular, podemos considerar $L_E(s)$ como una función analítica alrededor del punto $s = 1$.

El número $N$ que aparece en la conjetura 1 es un invariante muy importante de la curva elíptica $E$. Se llama **conductor de** $E$, y puede ser definido sin referirnos a ninguna conjetura. Es de la forma

$$\prod_p p^{e_p},$$

donde el producto es sobre los primos $p$ de mala reducción. Para la definición de $e_p$ ver [SIL], Apéndice C.

## 6.3 Conjetura de Shimura-Taniyama-Weil.

En esta sección vamos a enunciar una de las conjeturas más importantes en la teoría de curvas elípticas. Antes de ello daremos algunas definiciones y resultados.

Sea $SL_2(\mathbb{Z})$ el grupo formado por las matrices $2 \times 2$ con coeficientes enteros y determinante igual a 1. Este grupo actua sobre $\mathbb{P}^1(\mathbb{C})$ mediante:

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \longmapsto gz = \frac{az+b}{cz+d}.$$

El elemento $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ actúa como la identidad. Por tanto la acción factoriza a traves de $\{\pm I\}$ y podemos definir una acción del grupo $\Gamma = SL_2(\mathbb{Z})\Big/\{\pm I\}$

[1] Ver la siguiente sección.

sobre $\mathbb{P}^1(\mathbb{C})$. A $\Gamma$ se le denomina **grupo modular**. Se puede ver que $\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}$ es estable bajo la acción de $\Gamma$. Ahora consideramos el subgrupo de $\Gamma$ siguiente

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \bmod N \right\}.$$

**Proposición 6.3.1**

*(i) El espacio cociente* $Y_0(N) = \Gamma_0(N) \backslash \mathbb{H}$ *tiene estructura de variedad diferenciable no compacta de dimensión 1.*

*(ii) El compactificado de* $Y_0(N)$*, que denotaremos por* $X_0(N)$*, tiene estructura de superficie de Riemann compacta.*

*Demostración:* Ver [KNA], Capítulo XI, Sección 2.

**Conjetura de Shimura-Taniyama-Weil.** *Sea* $E$ *una curva elíptica definida sobre* $\mathbb{Q}$*. Entonces existe un entero* $N$ *y una aplicación racional no constante*

$$\phi : X_0(N) \longrightarrow E$$

*definida sobre* $\mathbb{Q}$*.*

Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$ tal que $E$ es la imagen racional de $X_0(N)$, para algún $N$; es decir, tal que $E$ cumple la conjetura de Shimura-Taniyama-Weil, entonces diremos que $E$ es una **curva elíptica modular** o **curva de Weil**.

Esta conjetura es una de las más importantes junto con la de Birch-Swinnerton-Dyer, que veremos en la sección siguiente, en la teoría de curvas elípticas. Para resaltar la potencia de esta conjetura tenemos el siguiente resultado publicado en [RIB].

**Teorema (Frey, Serre, Ribet).** *La conjetura de Shimura-Taniyama-Weil implica el Último Teorema de Fermat.*

Wiles ha demostrado la conjetura de Shimura-Taniyama-Weil para una gran cantidad de curvas elípticas y con ello demostró el Último Teorema de Fermat.

## 6.4 Conjetura de Birch-Swinnerton-Dyer.

La otra conjetura fundamental sobre curvas elípticas fue propuesta por Birch y Swinnerton-Dyer despues de hacer una gran cantidad de cálculos computacionales en curvas elípticas ([B-S-D]).

**Conjetura de Birch-Swinnerton-Dyer.** *Sea* $E$ *una curva elíptica definida sobre* $\mathbb{Q}$ *y supongamos cierta la conjetura 1 para* $E$*. Entonces si denotamos por* $r$ *el rango de* $E(\mathbb{Q})$*, se tiene que*

$$ord_{s=1} L_E(s) = r.$$

*Además,*

$$\lim_{s\to 1}\frac{L_E(s)}{(s-1)^r}=\Omega\frac{|Ш_E|R_E}{|E(\mathbb{Q})_{tors}|^2}\prod_{p\,|\,\Delta}c_p$$

*donde* $\Omega$ *es una constante fija,* $R_E$ *es el regulador de* $E$*,* $c_p$ *es un entero y* $Ш_E$ *es el objeto más misterioso, llamado* **grupo de Tate-Shafarevich de** $E$*.*

(Para una explicación detallada de las constantes que aquí aparecen, ver [SIL], Capítulo X, Sección 4).

$Ш_E$ es un grupo muy importante asociado a $E$. Está en conexión con el problema de calcular el rango de una curva elíptica dada. Se conjetura que $Ш_E$ es finito, pero hasta hace poco tiempo no se conocía ningún caso el que esto fuera cierto.

**Observación 6.4.1** Si pudiéramos encontrar una cota efectiva para $|Ш_E|$, una consecuencia sería la existencia de un algoritmo finito para determinar el rango de $E(\mathbb{Q})$ para cualquier curva elíptica $E$ definida sobre $\mathbb{Q}$.

También hay que resaltar la siguiente observación hecha por Mestre ([MES6]): si suponemos ciertas las conjeturas de Shimura-Taniyama-Weil, Birch-Swinnerton-Dyer y cierta forma de la hipótesis de Riemann, podemos dar un algoritmo para calcular el rango de una curva elíptica dada.

En 1972, Tate hizo el siguiente comentario en torno a la conjetura de Birch-Swinnerton-Dyer:

"Esta destacada conjetura relaciona el comportamiento de una función $L$ donde no se sabe que esté definida, con el orden de un grupo $Ш_E$, que no se sabe si es finito".

La conjetura de Birch-Swinnerton-Dyer ha sido verificada en una gran cantidad de casos, pero pocos resultados se han obtenido en torno a ella, hasta hace pocos años.

En lo que sigue, $E$ es una curva elíptica definida sobre $\mathbb{Q}$.

**Teorema (Coates-Wiles, 1977).** *Si* $E$ *tiene multiplicación compleja, entonces* $L_E(1)\neq 0$ *implica que* $E(\mathbb{Q})$ *es finito.*

**Teorema (Gross-Zagier, 1986).** *Si* $E$ *es una curva elíptica modular y* $L_E(s)$ *tiene un cero simple en* $s=1$*, entonces* $E(\mathbb{Q})$ *es infinito.*

**Teorema (Rubin, 1987).**

*(i) Si* $E$ *tiene multiplicación compleja y* $L_E(1)\neq 0$*, entonces* $Ш_E$ *es finito.*

*(ii) Si* $E$ *tiene multiplicación compleja y el rango de* $E(\mathbb{Q})$ *es* $\geq 2$*, entonces* $L_E(s)$ *tiene un cero en* $s=1$ *de orden* $\geq 2$*.*

El apartado (i) del anterior teorema fue el primer resultado en el que se demostró que el grupo de Tate-Shafarevich era finito para alguna curva elíptica.

**Teorema (Kolyvagin, 1988).** *Si $E$ tiene multiplicación compleja o es modular, y $ord_{s=1}L_E(s) \leq 1$, entonces*

$$rango\, E(\mathbb{Q}) = ord_{s=1}L_E(s).$$

En la actualidad, para rango mayor o igual a 2 poco se conoce acerca de la conjetura de Birch–Swinnerton-Dyer.

También hay otras conjeturas acerca del rango de las curvas elípticas; una de las más importantes es la siguiente:

**Conjetura 2.** *Existen curvas elípticas definidas sobre $\mathbb{Q}$ de rango arbitrariamente grande.*

La principal evidencia para que esta conjetura tenga sentido proviene del trabajo de Tate y Shafarevich ([SH-T]). Ellos mostraron que el resultado análogo es cierto para cuerpos de funciones (es decir, cuando $\mathbb{Q}$ es reemplazado por el cuerpo de funciones racionales $\mathbb{F}_p(T)$).

El actual récord es debido a Fermigier ([FE2]), que ha obtenido una curva elíptica de rango al menos 22. Sobre curvas elípticas de rango alto trataremos en el capítulo siguiente.

# Capítulo 7

# Curvas elípticas de rango alto.

Uno de los mayores problemas en la Teoría aritmética de curvas elípticas es el determinar una cota superior para el $K$-rango de curvas elípticas definidas sobre un cuerpo de números $K$. Se supone que esta cota superior es infinito. Este problema es de particular interés cuando $K = \mathbb{Q}$. En 1954, Nerón ([NER2]) mostró que existen infinitas curvas elípticas definidas sobre $\mathbb{Q}$ de rango $\geq 11$. Sin embargo, su método no era constructivo. Mediante el uso de computadoras se han obtenido varios ejemplos de curvas elípticas de rango alto. En las dos últimas décadas se han conseguido las siguiente curvas elípticas definidas sobre $\mathbb{Q}$:

| | | |
|---|---|---|
| Penny y Pomerance [P-P1] | 1974 | rango $\geq 6$, |
| Penny y Pomerance [P-P2] | 1975 | rango $\geq 7$, |
| Grunewald y Zimmert [G-ZI] | 1977 | rango $\geq 8$, infinitos ejemplos, |
| Brumer y Kramer [B-K] | 1977 | rango $\geq 9$, |
| Nishioka [NIS] | 1979 | rango $\geq 9$, infinitos ejemplos, |
| Mestre [MES5] | 1982 | rango $\geq 12$, |
| Mestre [MES4] | 1986 | rango $\geq 14$, |
| Mestre [MES3] | 1991 | rango $\geq 15$, |
| Nagao [NA1] | 1992 | rango $\geq 17$, |
| Tunnel (sin publicar) | 1992 | rango $\geq 18$, |
| Fermigier [FE1] | 1992 | rango $\geq 19$, |
| Nagao [NA2] | 1993 | rango $\geq 20$, |
| Nagao y Kouya [N-K] | 1994 | rango $\geq 21$, |
| Fermigier [FE2] | 1996 | rango $\geq 22$. |

Y sobre $\mathbb{Q}(T)$:

| | | |
|---|---|---|
| Mestre [MES1] | 1991 | rango $\geq 11$, |
| Mestre [MES2] | 1991 | rango $\geq 12$, |
| Nagao [NA3] | 1993 | rango $\geq 13$, |
| Mestre [MES7] | 1995 | rango $\geq 13$, infinitos ejemplos, |
| (en concreto esta curva está definida sobre $\mathbb{Q}(u, v)(T)$) | | |
| Mestre (sin publicar) | 1996 | rango $\geq 14$, infinitos ejemplos. |

En la sección §7.7 veremos los ejemplos obtenidos por Nagao y Kouya ([N-K])

y el de Fermigier ([FE2]), que es el actual récord. También explicaremos todos los ejemplos publicados definidos sobre $\mathbb{Q}(T)$ que hemos mencionado. Estos últimos ejemplos son de particular interés ya que tienen invariante $j$ no constante, es decir, obtendremos familias infinitas de curvas elípticas, no isomorfas entre sí, definidas sobre $\mathbb{Q}$ de rango alto.

En las secciones §7.6.1 y §7.6.2 discutiremos los métodos de Mestre ([MES1] y [MES2]), debido a que son básicos en la obtención de curvas elípticas de rango alto. En particular, discutiremos el método desarrollado en §7.6.2.

Sea $p$ un número primo. Una curva elíptica $E$ tiene buena reducción en $p$ si $p \not| \Delta$. Para una curva elíptica $E$ definida sobre $\mathbb{Q}$ y un entero positivo $N$, Mestre define

$$s_{Mestre}(N, E) := \sum_{\substack{p \leq N \\ p \not| \Delta}} \left( \frac{p-1}{|E_p(\mathbb{F}_p)|} - 1 \right) \cdot log\, p,$$

donde $|E_p(\mathbb{F}_p)|$ es el número de puntos $\mathbb{F}_p$-racionales de $E$. Entonces Mestre encuentra curvas elípticas de rango alto entre curvas elípticas con $s_{Mestre}(N, E)$ grande, para un cierto $N$.

Nagao ([NA2] y [NA5]) mejora la criba $s_{Mestre}(N, E)$, introduciendo

$$s_{Nagao}(N, E) := -\frac{1}{N} \sum_{\substack{p \leq N \\ p \not| \Delta}} a_p(E) \cdot log\, p,$$

donde $a_p(E) = p + 1 - |E_p(\mathbb{F}_p)|$ si $E_p$ es una curva elíptica y $a_p(E_p) = \epsilon_p(E)$ si no.

Para obtener curvas elípticas de rango alto sobre $\mathbb{Q}$ seguiremos los siguientes pasos:

(i) Construimos curvas elípticas $\mathcal{E}$ definidas sobre $\mathbb{Q}(T)$ con rango $\geq 11$ por el método de Mestre discutido en la sección §7.6.2.

(ii) Entre las curvas definidas sobre $\mathbb{Q}$ obtenidas por especialización de $\mathcal{E}$, elegimos las curvas elípticas $\mathcal{E}_t$ tales que $s_{Nagao}(N, \mathcal{E}_t)$ sea grande para un cierto $N$.

(iii) Buscamos puntos racionales en las curvas elípticas obtenidas en (ii) y encontramos puntos racionales independientes.

Con este procedimiento, Mestre ([MES3]) construye una curva elíptica definida sobre $\mathbb{Q}$ de rango $\geq 15$ , posteriormente [NA1] construye una de rango $\geq 17$ y después Tunnel una de rango $\geq 18$. Así hasta llegar a la curva de rango $\geq 21$ obtenida por Nagao y Kouya ([N-K]). El actual récord es debido a Fermigier ([FE2]), que ha construido una curva elíptica definida sobre $\mathbb{Q}$ con rango $\geq 22$ a partir de una curva elíptica definida sobre $\mathbb{Q}(u, v)(T)$ de rango $\geq 13$ obtenida previamente por Mestre ([MES7]).

Para encontrar curvas elípticas definidas sobre $\mathbb{Q}(T)$ de rango alto, Nagao define $S(N, \mathcal{E})$, una nueva criba, para una curva elíptica $\mathcal{E}$ definida sobre $\mathbb{Q}(T)$ y para un entero positivo $N$. Supongamos que $\mathcal{E}$ está definida por una ecuación de Weierstrass con coeficientes en $\mathbb{Z}[T]$. Denotaremos por $\mathcal{E}_t$ a la curva elíptica obtenida de $\mathcal{E}$ mediante la especialización $\sigma_t : T \longmapsto t$ $(t \in \mathbb{Z})$. Para un número primo $p$, tenemos

$$A_p(\mathcal{E}) = \frac{1}{p} \sum_{t=0}^{p-1} a_p(\mathcal{E}_t),$$

donde $a_p(\mathcal{E}_t) = p + 1 - |\mathcal{E}_t(\mathbb{F}_p)|$ y $|\mathcal{E}_t(\mathbb{F}_p)|$ es el número de puntos $\mathbb{F}_p$-racionales en $\mathcal{E}_t$ incluido el punto del infinito, si $\mathcal{E}_t$ es una curva elíptica y si no, $a_p(\mathcal{E}_t) = \epsilon_p(\mathcal{E}_t)$. Entonces la criba $S(N, \mathcal{E})$ está definida por

$$S(N, \mathcal{E}) := -\frac{1}{N} \sum_{p \leq N} A_p(\mathcal{E}) \cdot log\, p.$$

Usando $S(N, \mathcal{E})$, Nagao ([NA3]) encuentra una curva elíptica definida sobre $\mathbb{Q}(T)$ de rango 13. Además, Nagao observó mediante experimentos computacionales que $S(N, \mathcal{E})$ converge al rango de $\mathcal{E}(\mathbb{Q}(T))$ cuando $N \to \infty$. Es decir,

**Conjetura de Nagao.**

$$rango\, \mathcal{E}(\mathbb{Q}(T)) = \lim_{N \to \infty} S(N, \mathcal{E}).$$

El propio Nagao ([NA4]) la demuestra para ciertos casos particulares de superficies elípticas. Y Silvermann y Rosen ([SIL3] y [R-S]) amplían la demostración para un mayor número de superficies elípticas.

## 7.1 La criba $s_{Nagao}(N, E)$ para curvas elípticas sobre $\mathbb{Q}$.

Para una curva elíptica $E$ definida sobre $\mathbb{Q}$ y un entero positivo $N$, definimos la criba

$$s_{Nagao}(N, E) = -\frac{1}{N} \sum_{\substack{p \leq N \\ p \nmid \Delta}} a_p(E) \cdot log\, p.$$

Vamos a ver por qué el valor

$$\lim_{N \to \infty} s_{Nagao}(N, E) + \frac{1}{2}$$

puede ser usado como una medida para obtener curvas elípticas de rango alto. Para llegar a este fin, asumiremos la conjetura de Birch-Swinnerton-Dyer y la conjetura

de Sato-Tate, que veremos más adelante. La primera establece que el rango de una curva elíptica $E$ definida sobre $\mathbb{Q}$ es igual al orden del cero de su función $L_E(s)$ en $s = 1$, donde

$$L_E(s) = \prod_{p \mid \Delta} (1 - \epsilon_p(E)p^{-s})^{-1} \prod_{p \nmid \Delta} (1 - a_p(E)p^{-s} + p^{1-2s})^{-1}.$$

Reescribiendo la conjetura de Birch-Swinnerton-Dyer tenemos que

$$rango\, E(\mathbb{Q}) = res_{s=1} \frac{L'_E(s)}{L_E(s)}.$$

Por otra parte, escribimos

$$\begin{aligned} &1 - a_p(E)T + pT^2 = (1 - \alpha_p T)(1 - \overline{\alpha_p} T), \\ &b(p, m) = \alpha_p^m + \overline{\alpha_p}^m \end{aligned}$$

y

$$f_m(s) = -\sum_{p \nmid \Delta} log\, p \cdot b(p, m) \cdot p^{-ms}.$$

Vamos a demostrar la siguiente igualdad, válida en el semiplano $Re(s) > \frac{3}{2}$:

$$\frac{L'_E(s)}{L_E(s)} = -\sum_{m=1}^{\infty} f_m(s) + \sum_{p \mid \Delta} \frac{-\epsilon_p(E) \cdot log\, p \cdot p^{-s}}{1 - \epsilon_p(E) \cdot p^{-s}}.$$

Se comprueba facílmente que

$$\frac{L'_E(s)}{L_E(s)} = -\left[ \sum_{p \mid \Delta} \left( log(1 - \epsilon_p(E)p^{-s}) \right)' + \sum_{p \nmid \Delta} \left( log(1 - a_p(E)p^{-s} + p^{1-2s}) \right)' \right].$$

Por lo tanto, sólo nos queda ver si

$$\sum_{m=1}^{\infty} f_m(s) = \sum_{p \nmid \Delta} \left( log(1 - a_p(E)p^{-s} + p^{1-2s}) \right)'.$$

Para demostrar esta igualdad, vamos a usar el teorema de Hasse, que nos dice que $|\alpha_p| = p^{1/2}$. Con esto obtenemos $|b(p, m)| \leq 2p^{m/2}$. Veamos a continuación la igualdad. Vamos a hacerlo por partes:

(i) Se tiene

$$log(1 - a_p(E)p^{-s} + p^{1-2s}) = log\left( (1 - \alpha_p p^{-s})(1 - \overline{\alpha_p} p^{-s}) \right).$$

Si $|\alpha_p| p^{-Re(s)} < 1$, es decir, si $Re(s) > \frac{1}{2}$ obtenemos

$$log(1 - a_p(E)p^{-s} + p^{1-2s}) = \sum_{n=1}^{\infty} \frac{\alpha_p^n}{np^{ns}} + \sum_{n=1}^{\infty} \frac{\overline{\alpha_p}^n}{np^{ns}} = \sum_{n=1}^{\infty} \frac{b(p, n)}{n} p^{-ns}.$$

(ii) Queremos derivar el sumatorio anterior y para ello vamos a utilizar el criterio M de Weierstrass para la serie de funciones holomorfas $F_m(s) = \dfrac{b(p,m)}{m} p^{-ms}$ en el semiplano $Re(s) > \frac{3}{2}$. Se tiene que $|F_m(s)| \leq M_m = \dfrac{1}{mp^m}$, y como $\displaystyle\sum_{m=1}^{\infty} M_m < \infty$, obtenemos

$$\big(log(1 - a_p(E)p^{-s} + p^{1-2s})\big)' = -\sum_{n=1}^{\infty} b(p,n) \cdot log\, p \cdot p^{-ns}.$$

(iii) Queremos intercambiar el orden de sumación en

$$\sum_{p \nmid \Delta} \sum_{m=N}^{\infty} log\, p \cdot b(p,m) \cdot p^{-ms} \qquad N \geq 1. \tag{7.1}$$

Para ello vamos a ver que la serie anterior define una función holomorfa en el semiplano $Re(s) > \frac{1}{2} + \frac{1}{N}$.

- $\displaystyle\sum_{m=N}^{\infty} b(p,m) \cdot p^{-ms}$ es una función holomorfa en $Re(s) > \frac{1}{2} + \frac{1}{N}$, ya que $b(p,m) \cdot p^{-ms}$ es holomorfa, $|b(p,m) \cdot p^{-ms}| \leq M_m = 2p^{-m/N}$ para todo $m \geq N$ y $\displaystyle\sum_{m=N}^{\infty} M_m < \infty$.
- La función $G_p(s) = \displaystyle\sum_{m=N}^{\infty} log\, p \cdot b(p,m) \cdot p^{-ms}$ es holomorfa en $Re(s) > \frac{1}{2} + \frac{1}{N}$ para todo $p \nmid \Delta$. Además, $\forall p \nmid \Delta$

  $$|G_p| \leq 2 \sum_{m=N}^{\infty} log\, p \cdot p^{-m(Re(s)-\frac{1}{2})} = \frac{2 \cdot log\, p}{p^{(Re(s)-\frac{1}{2})N} - p^{(Re(s)-\frac{1}{2})(N-1)}} = M'_p.$$

  Como $\displaystyle\sum_{p \nmid \Delta}^{\infty} M'_p < \frac{2^{1/N}}{2^{1/N} - 1} \sum_{p \nmid \Delta} \frac{2 \cdot log\, p}{p^{(Re(s)-\frac{1}{2})N}} < \infty$ si $Re(s) > \frac{1}{2} + \frac{1}{N}$, el criterio $M$ de Weierstrass nos asegura que (7.1) es una función holomorfa en el semiplano $Re(s) > \frac{1}{2} + \frac{1}{N}$; y podremos intercambiar el orden de sumación.

Con esto hemos obtenido los siguientes resultados:

- Si $Re(s) > \frac{3}{2}$, entonces,

  $$\sum_{p \nmid \Delta} \sum_{m=1}^{\infty} log\, p \cdot b(p,m) \cdot p^{-ms} = \sum_{m=1}^{\infty} \sum_{p \nmid \Delta} log\, p \cdot b(p,m) \cdot p^{-ms} = \sum_{m=1}^{\infty} f_m(s),$$

  que es lo que queríamos demostrar.

- Además, si $Re(s) > \frac{5}{6}$, entonces la serie

$$\sum_{m=3}^{\infty} f_m(s)$$

converge a una función holomorfa.

Por lo tanto hemos demostrado que

$$\frac{L'_E(s)}{L_E(s)} = -\sum_{m=1}^{\infty} f_m(s) + \sum_{p \mid \Delta} \frac{-\epsilon_p(E) log\, p \cdot p^{-s}}{1 - \epsilon_p(E) p^{-s}} \qquad Re(s) > \frac{3}{2}. \tag{7.2}$$

**Proposición 7.1.1** *Sea* $f(s) = \sum_{n=1}^{\infty} a_n\, n^{-s}$ *con* $a_n \in \mathbb{C}$*, una serie de Dirichlet que converge en* $Re(s) > \sigma > 1$*. Si el límite*

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n \leq N} a_n$$

*existe, entonces* $f(s)$ *converge en* $Re(s) > 1$ *y*

$$\lim_{s \to 1^+} (s-1) \cdot f(s) = \lim_{N \to \infty} \frac{1}{N} \sum_{n \leq N} a_n.$$

*Demostración:* La fórmula de sumación por partes de Abel nos dice

$$\sum_{k \leq N} \frac{a_k}{k^s} = \sum_{k < N} \left( \sum_{n \leq k} a_n \right) \left( \frac{1}{k^s} - \frac{1}{(k+1)^s} \right) + \frac{1}{N^s} \sum_{n \leq N} a_n.$$

Por otra parte, denontando $\sigma = Re(s)$, el teorema del valor medio nos dice que existe $\xi_k$ con $k < \xi_k < k+1$, tal que

$$\frac{1}{k^\sigma} - \frac{1}{(k+1)^\sigma} = \frac{\sigma}{\xi_k^{\sigma+1}}. \tag{7.3}$$

Utilizando que el limite de $\frac{1}{N} \sum_{k \leq N} a_k$ existe, podemos conseguir una constante $C$ tal que

$$\left| \sum_{k \leq N} a_k \right| \leq CN.$$

Por lo tanto, juntando todo lo anterior,

$$\sum_{k \leq N} \left| \frac{a_k}{k^s} \right| \leq \sum_{k < N} \frac{C' |\sigma|}{k^\sigma} + o(1).$$

Entonces $f(s)$ converge en $\sigma = Re(s) > 1$.

Ahora vamos a probar que si $\lim_{N\to\infty} \frac{1}{N}\sum_{k\leq N} a_k = l$, entonces $\lim_{s\to 1}(s-1)f(s) = l$.

Se deduce la siguiente identidad

$$f(\sigma) = \sum_{k=1}^{\infty}\left(\frac{1}{k}\sum_{n\leq k} a_n\right) k\left(\frac{1}{k^\sigma} - \frac{1}{(k+1)^\sigma}\right) = \sum_{k=1}^{\infty} F_k(\sigma).$$

Utilizando (7.3),

$$k^\sigma F_k(\sigma) = \sigma\left(\frac{k}{\xi_k}\right)^{\sigma+1}\left(\frac{1}{k}\sum_{n\leq k} a_n\right).$$

Como $\lim_{N\to\infty} \frac{1}{N}\sum_{k\leq N} a_k = l$, $\forall\,\varepsilon > 0$, $\exists M = M(\varepsilon)$ tal que

$$|k^\sigma F_k(\sigma) - \sigma l| < \varepsilon \quad \text{para } k > M.$$

Y con esto obtendremos

$$\sum_{k>M}\left|F_k(\sigma) - \frac{\sigma l}{k^\sigma}\right| < \sum_{k>M}\frac{\varepsilon}{k^\sigma}. \tag{7.4}$$

Entonces, por lo anterior

$$\begin{aligned}\left|\sum_{k=1}^{\infty}\left(F_k(\sigma) - \frac{\sigma l}{k^\sigma}\right)\right| &\leq \left|\sum_{k\leq M}\left(F_k(\sigma) - \frac{\sigma l}{k^\sigma}\right)\right| + \left|\sum_{k>M}\left(F_k(\sigma) - \frac{\sigma l}{k^\sigma}\right)\right| &(7.5)\\ &\leq \left|\sum_{k\leq M}\left(F_k(\sigma) - \frac{\sigma l}{k^\sigma}\right)\right| + \sum_{k>M}\frac{\varepsilon}{k^\sigma} &(7.6)\\ &\leq \left|\sum_{k\leq M}\left(F_k(\sigma) - \frac{\varepsilon + \sigma l}{k^\sigma}\right)\right| + \sum_{k=1}^{\infty}\frac{\varepsilon}{k^\sigma} &(7.7)\end{aligned}$$

Si denotamos por $\zeta(s) = \sum_{k=1}^{\infty}\frac{1}{k^s}$, la función $\zeta$ de Riemann, obtenemos

$$|f(\sigma)(\sigma-1) - \sigma l(\sigma-1)\zeta(\sigma)| \leq (\sigma-1)\left|\sum_{k\leq M}\left(F_k(\sigma) - \frac{\varepsilon+\sigma l}{k^\sigma}\right)\right| + (\sigma-1)\zeta(\sigma)\varepsilon,$$

y como $\lim_{\sigma\to 1^+}(\sigma-1)\zeta(\sigma) = 1$, concluimos que

$$\lim_{\sigma\to 1^+}(\sigma-1)f(\sigma) = l,$$

que es lo que queriamos.

□

Es fácil ver que

$$f_1(s) = -\sum_{p \not| \Delta} log\, p \cdot a_p(E) \cdot p^{-s}.$$

Suponiendo la existencia de $\lim_{N\to\infty} s_{Nagao}(N, E)$ tendríamos, por la proposición anterior, que $f_1(s)$ es holomorfa en $Re(s) > 1$. Además, la función $f_2(s)$ también es holomorfa en $Re(s) > 1$, por tanto, la parte derecha de la identidad (7.2) define una función holomorfa en $Re(s) > 1$. Al suponer cierta la conjetura de Birch-Swinnerton-Dyer, hemos admitido que $L_E(s)$ tiene una continuación analítica en todo el plano a una función meromorfa. Con lo que concluimos que la identidad (7.2) es válida en $Re(s) > 1$.

Calculemos el residuo de $\dfrac{L'_E(s)}{L_E(s)}$ en $s = 1$. Las funciones

$$\sum_{p \mid \Delta} \frac{-\epsilon_p(E) log\, p \cdot p^{-s}}{1 - \epsilon_p(E)p^{-s}} \quad \text{y} \quad \sum_{m=3}^{\infty} f_m(s)$$

son holomorfas en $Re(s) > \frac{5}{6}$. Por lo tanto,

$$res_{s=1}\frac{L'_E(s)}{L_E(s)} = res_{s=1} f_1(s) + res_{s=1} f_2(s).$$

Utilizando de nuevo la proposición anterior, y bajo la suposición de la existencia de $\lim_{N\to\infty} s_{Nagao}(N, E)$, obtenemos

$$\lim_{s\to 1^+} (s-1) \cdot f_1(s) = \lim_{N\to\infty} -\frac{1}{N} \sum_{\substack{p \le N \\ p \not| \Delta}} a_p(E) \cdot log\, p.$$

Es decir,

$$\boxed{Res_{s=1} f_1(s) = \lim_{N\to\infty} s_{Nagao}(N, E)}.$$

Ahora vamos a calcular el residuo de $f_2(s)$. Para ello, asumiremos la conjetura de Sato-Tate. Pero antes de enunciarla debemos de dar algunas definiciones. Dada $E$ una curva elíptica definida sobre $\mathbb{Q}$, definimos

$$c_m = \lim_{N\to\infty} \frac{1}{\pi(N)} \sum_{\substack{p \le N \\ p \not| \Delta}} \frac{b(p, m)}{p^{m/2}}, \qquad m \ge 1,$$

donde $\pi(N)$ es el número de primos menores que un entero positivo $N$.

Utilizando el teorema de los números primos (ver [C-C], Capítulo 1) y la Proposición 1.8 de [C-C], deducimos

$$\lim_{N\to\infty} \frac{\pi(N)}{N/log\, N} = \lim_{N\to\infty} \frac{1}{N} \sum_{p\leq N} log\, p = 1. \tag{7.8}$$

Con esto, vamos a probar que

$$c_m = \lim_{N\to\infty} \frac{1}{N} \sum_{\substack{p \leq N \\ p\not| \Delta}} log\, p \cdot \frac{b(p,m)}{p^{m/2}}, \qquad m \geq 1.$$

Es decir, probaremos

$$\lim_{N\to\infty} \sum_{p\leq N} \frac{b(p,m)}{p^{m/2}} \left\{ \frac{1}{\pi(N)} - \frac{log\, p}{N} \right\} = 0.$$

Utilizando el teorema de los números primos deducimos $\frac{1}{\pi(N)} = \frac{log\, N}{N} - o\left(\frac{log\, N}{N}\right)$; y junto con (7.8) y con $|b(p,m)| \leq 2p^{m/2}$, obtenemos

$$\begin{aligned} &\left| \sum_{p\leq N} \frac{b(p,m)}{p^{m/2}} \left\{ \frac{1}{\pi(N)} - \frac{log\, p}{N} \right\} \right| \leq 2 \sum_{p\leq N} \left| \frac{\log\, N}{N} + o\left(\frac{log\, N}{N}\right) - \frac{log\, p}{N} \right| \\ &\leq \pi(N) \frac{log\, N}{N} - \frac{1}{N} \sum_{p\leq N} log\, p + \pi(N)\, o\left(\frac{log\, N}{N}\right) \longrightarrow 0 \quad \text{si } N \to \infty. \end{aligned}$$

Entonces la conjetura de Sato-Tate se enuncia (ver [TAT], página 106) de la siguiente forma:

**Conjetura de Sato-Tate.** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$ sin multiplicación compleja. Entonces para $m \geq 1$,*

$$c_m = \begin{cases} -1 & si\ m = 2, \\ 0 & si\ m \neq 2. \end{cases}$$

Para completar nuestro cálculo al caso de curvas elípticas con multiplicación compleja utilizaremos el siguiente teorema debido a Nagao ([NA5]).

**Teorema 7.1.2** *Sea $E$ una curva elíptica definida sobre $\mathbb{Q}$ con multiplicación compleja. Entonces, para $m \geq 1$ se tiene que*

$$c_m = \begin{cases} (-1)^k & si\ m = 2k, \\ 0 & si\ m = 2k-1. \end{cases}$$

*Demostración:* Ver [NA5], Lema 2.1.

Ya estamos en disposición de calcular el residuo de $f_2(s)$ en $s = 1$.

**Proposición 7.1.3** *Asumiendo la conjetura de Sato-Tate, se tiene que*

$$\lim_{s\to 1^+} (s-1)\cdot f_2(s) = \frac{1}{2}.$$

*Demostración:* Tenemos

$$-1 = c_2 = \lim_{N\to\infty} \frac{1}{N} \sum_{\substack{p \leq N \\ p\not| \Delta}} log\, p \cdot \frac{b(p,2)}{p},$$

y denotemos

$$g(s) = \sum_{p\not| \Delta} \frac{log\, p \cdot b(p,2)}{p}\, p^{-s}.$$

Utilizando la proposición 7.1.1 obtenemos:

$$\lim_{s\to 1^+} (s-1)\cdot g(s) = -1.$$

Por otra parte,

$$f_2(s) = -g(2s-1),$$

y entonces,

$$\lim_{s\to 1^+} (s-1)\cdot f_2(s) = \lim_{s\to 1^+} -(s-1)\cdot g(2s-1) = \frac{1}{2}.$$

□

Por lo tanto hemos obtenido que, asumiendo las conjeturas de Birch-Swinnerton-Dyer y de Sato-Tate junto con la suposición de la existencia de $\lim_{N\to\infty} s_{Nagao}(N,E)$ se tiene

$$\boxed{rango\, E(\mathbb{Q}) = \lim_{N\to\infty} s_{Nagao}(N,E) + \frac{1}{2}.}$$

De ahí que $s_{Nagao}(N,E)$ sea una buena aproximación del rango de $E(\mathbb{Q})$. Con esto, si encontramos curvas elípticas $E$ sobre $\mathbb{Q}$ que tengan $s_{Nagao}(N,E)$ grande, para un cierto $N$, obtendremos que probablemente su rango será alto; y en la práctica es lo que ocurre, como veremos en la última sección de este capítulo.

## 7.2 Superficies elípticas.

En esta sección vamos a hacer un breve estudio sobre la teoría de superficies elípticas, que nos será necesaria para estudiar curvas elípticas definidas sobre $\mathbb{Q}(T)$, que abordaremos en las próximas secciones.

**Definición.** *Sea $C$ una curva proyectiva lisa definida sobre un cuerpo $K$. Una* **superficie elíptica sobre** *$C$ consiste en:*

*(i) Una superficie $\mathcal{E}$.*

*(ii) Un morfismo*

$$\pi : \mathcal{E} \longrightarrow C,$$

*tal que para todo punto $t \in C(\overline{K})$, excepto un número finito de ellos, la* **fibra** *$\mathcal{E}_t := \pi^{-1}(t)$ es una curva lisa de género 1.*

*(iii) Una sección de $\pi$,*

$$\sigma_0 : C \longrightarrow \mathcal{E}.$$

*Es decir, $\pi \circ \sigma_0 \sim id_C$.*

Sea $\mathcal{E} \longrightarrow C$ una superficie elíptica. El **grupo de secciones de $\mathcal{E}$ sobre** $C$ se denota por

$$\mathcal{E}(C) := \{\sigma : C \longrightarrow \mathcal{E} : \pi \circ \sigma \sim id_C\}.$$

Diremos que una superficie elíptica $\mathcal{E}$ sobre $C$ está **definida sobre** $K$ si la curva, la superficie $\mathcal{E}$ y las aplicaciones $\pi$ y $\sigma_0$ están definidas sobre $K$. En este caso escribiremos

$$\mathcal{E}(C/K) := \{\sigma \in \mathcal{E}(C) : \sigma \text{ está definida sobre } K\}.$$

**Definición.** *Sean $\pi : \mathcal{E} \longrightarrow C$ y $\pi' : \mathcal{E}' \longrightarrow C$ superficies elípticas sobre $C$. Una* **aplicación racional de $\mathcal{E}$ a $\mathcal{E}'$ sobre** *$C$ es una aplicación racional $\phi : \mathcal{E} \longrightarrow \mathcal{E}'$ tal que $\pi' \circ \phi = \pi$.*

*Las superficies elípticas $\mathcal{E}$ y $\mathcal{E}'$ son* **birracionalmente equivalentes sobre** *$C$ si existe una aplicación birracional $\phi : \mathcal{E} \longrightarrow \mathcal{E}'$. Si las superficies elípticas y las aplicaciones racionales están definidas sobre un cuerpo $K$, diremos que $\mathcal{E}$ y $\mathcal{E}'$ son* **$K$-birracionalmente equivalentes sobre** *$C$.*

La siguiente proposición explica por qué la teoría de curvas elípticas definidas sobre un cuerpo de funciones $K(C)$ es la misma que la teoría birracional de superficies elípticas sobre $C$.

**Proposición 7.2.1** *(i) Fijada una curva elíptica $E$ definida sobre $K(C)$, a cada ecuación de Weierstrass de $E$ de la forma*

$$y^2 = x^3 + Ax + B \qquad A, B \in K(C)$$

*le asociamos una superficie elíptica*

$$\mathcal{E}(A, B) = \{([x, y, z], t) \in \mathbb{P}^2 \times C : y^2 z = x^3 + A(t)xz^2 + B(t)z^3\}.$$

*Entonces todas las superficies elípticas $\mathcal{E}(A, B)$ asociadas a $E$ son $K$-birracionalmente equivalentes sobre $C$.*

*(ii) Sea $\mathcal{E}$ una superficie elíptica sobre $C$ definida sobre $K$. Entonces $\mathcal{E}$ es $K$-birracionalmente equivalente sobre $C$ a $\mathcal{E}(A,B)$ para unos ciertos $A, B \in K(C)$. Además, la curva elíptica definida sobre $K(C)$*

$$E : y^2 = x^3 + Ax + B$$

*está unívocamente determinada, salvo $K(C)$-isomorfismos, por $\mathcal{E}$.*

*Diremos que $E/K(C)$ es la* **fibra genérica** *de $\mathcal{E} \longrightarrow C$.*

*Demostración:* Ver [SIL2], Capítulo III, Proposición 3.8.

Nuestro siguiente propósito es convertir $\mathcal{E}(C)$ en un grupo. Para ello, si $\sigma_1, \sigma_2 \in \mathcal{E}(C)$, definimos dos nuevas secciones $\sigma_1 \oplus \sigma_2$ y $\ominus\sigma_1$ por la regla

$$\begin{aligned}(\sigma_1 \oplus \sigma_2)(t) &= \sigma_1(t) + \sigma_2(t),\\ (\ominus\sigma_1)(t) &= -(\sigma_1(t)),\end{aligned}$$

para todo $t \in C$ tal que la fibra $\mathcal{E}_t$ es lisa.

**Proposición 7.2.2** *Sea $\mathcal{E} \longrightarrow C$ una superficie elíptica definida sobre $K$.*

*(i) Sean $\sigma_1, \sigma_2 \in \mathcal{E}(C/K)$. Entonces $\sigma_1 \oplus \sigma_2 \in \mathcal{E}(C/K)$ y $\ominus\sigma_1 \in \mathcal{E}(C/K)$.*

*(ii) Sea $E/K(C)$ la curva asociada a la superficie elíptica $\mathcal{E}$. Entonces la siguiente aplicación es un isomorfismo:*

$$\begin{array}{rcl} E(K(C)) & \longrightarrow & \mathcal{E}(C/K) \\ P = (x_P, y_P) & \longmapsto & (\sigma_P : t \mapsto (P_t, t)), \end{array}$$

*donde $P_t = (x_P(t), y_P(t))$.*

*(iii) Las operaciones*

$$\begin{array}{ccc} \mathcal{E}(C/K) \times \mathcal{E}(C/K) & \longrightarrow & \mathcal{E}(C/K) \\ (\sigma_1, \sigma_2) & \longmapsto & \sigma_1 \oplus \sigma_2 \end{array} \qquad \begin{array}{ccc} \mathcal{E}(C/K) & \longrightarrow & \mathcal{E}(C/K) \\ \sigma & \longmapsto & \ominus\sigma \end{array}$$

*hacen a $\mathcal{E}(C/K)$ un grupo abeliano.*

*Demostración:* Ver [SIL2], Capítulo III, Proposición 3.10.

Al igual que en el caso de curvas elípticas, vamos a conseguir un teorema de Mordell para un determinado tipo de superficies elípticas.

**Definición.** *Una superficie elíptica $\pi : \mathcal{E} \longrightarrow C$ se* **descompone sobre** *$K$ si existen una curva elíptica $E_0/K$ y un isomorfismo birracional $i : \mathcal{E} \longrightarrow E_0 \times C$ tales que si denotamos por $pr : E_0 \times C \longrightarrow C$, se tiene $pr \circ i = \pi$.*

**Teorema de Mordell-Weil para cuerpos de funciones.** *Sea $\mathcal{E} \longrightarrow C$ una superficie elíptica definida sobre un cuerpo $K$ y sea $E/K(C)$ su correspondiente curva elíptica definida sobre el cuerpo de funciones $K(C)$. Si $\mathcal{E} \longrightarrow C$ no se descompone sobre $K$, entonces $E(K(C))$ es un grupo abeliano finitamente generado.*

*Demostración:* Ver [SIL2], Capítulo III, Teorema 6.1.

## 7.3 Teoremas de especialización para superficies elípticas.

A partir de ahora "superficie elíptica"querrá decir superficie elíptica no descomponible. Sea $\mathcal{E} \longrightarrow C$ una superficie elíptica. Para cada punto $P \in E(K(C))$ definimos el morfismo

$$\begin{array}{rccc} \sigma_p: & C & \longrightarrow & \mathcal{E} \\ & t & \longmapsto & P_t. \end{array}$$

Por otro lado, cada punto $t \in C(\overline{K})$ determina una aplicación

$$\begin{array}{rccc} \sigma_t: & E(K(C)) & \longrightarrow & \mathcal{E}_t(\overline{K}), \\ & P & \longmapsto & P_t. \end{array}$$

llamada **especialización de $\mathcal{E}$ en** $t$.

**Proposición 7.3.1** *Si la fibra $\mathcal{E}_t$ es lisa, entonces la especialización $\sigma_t$ es un homomorfismo de grupos.*

*Demostración:* Queremos ver que $\sigma_t(P \oplus Q) = \sigma_t(P) \oplus \sigma_t(Q)$. Utilizando que $\sigma_{P\oplus Q}(t) = \sigma_P(t) \oplus \sigma_Q(t)$ si $\mathcal{E}_t$ es lisa obtenemos:

$$\sigma_t(P \oplus Q) = (P \oplus Q)_t = \sigma_{P\oplus Q}(t) = \sigma_P(t) + \sigma_Q(t) = P_t \oplus Q_t = \sigma_t(P) \oplus \sigma_t(Q). \square$$

**Proposición 7.3.2** *Sea $\mathcal{E} \longrightarrow C$ una superficie elíptica definida sobre $K$ y sea $t \in C(\overline{K})$ tal que $\mathcal{E}_t$ es lisa. Entonces, si los puntos $P_1, \ldots, P_k \in E(K(C))$ son dependientes en $E(K(C))$, los puntos $(P_1)_t, \ldots, (P_k)_t \in \mathcal{E}_t(\overline{K})$ serán dependientes en $\mathcal{E}_t(\overline{K})$.*

*Demostración:* Se sigue de que la especialización $\sigma_t$ es un homomorfismo de grupos si $\mathcal{E}_t$ es lisa.

$\square$

De hecho, se tiene el siguiente resultado:

**Teorema 7.3.3** *Sea $\mathcal{E} \longrightarrow C$ una superficie elíptica definida sobre un cuerpo de números $K$. Entonces,*

$$\begin{array}{rccc} \sigma_t: & E(K(C)) & \longrightarrow & \mathcal{E}_t(\overline{K}) \\ & P & \longmapsto & P_t, \end{array}$$

*es inyectiva para todo $t \in C(\overline{K})$, excepto para un número finito de $t \in C(\overline{K})$.*

*Demostración:* Ver [SIL2], Capítulo III, Teorema 11.4.

El caso que más nos va a interesar en las siguientes secciones es cuando $C = \mathbb{P}^1$ y $K = \mathbb{Q}$. Con esto tenemos que $K(C) = \mathbb{Q}(T)$ (ver observación 2.2.4). Tendremos curvas elípticas $E$ definidas sobre $\mathbb{Q}(T)$. Para obtener una cota inferior

del rango de $E(\mathbb{Q}(T))$ construiremos $n$ puntos $P_1, \ldots, P_n \in E(\mathbb{Q}(T))$ tales que mediante la especialización $\sigma_t$, para un cierto $t \in \mathbb{P}^1(\mathbb{Q})$, obtenemos $n$ puntos distintos $(P_1)_t, \ldots, (P_n)_t$. Así si $(P_1)_t, \ldots, (P_n)_t$ son independientes en $\mathcal{E}_t(\mathbb{Q})$, se tendrá que $P_1, \ldots, P_n$ son independientes en $E(\mathbb{Q}(T))$ y que por tanto $rango\, E(\mathbb{Q}(T)) \geq n$.

El teorema anterior nos dice que $\sigma_t : E(\mathbb{Q}(T)) \longrightarrow \mathcal{E}_t(\overline{\mathbb{Q}})$ es inyectiva para todo $t \in \mathbb{P}^1(\mathbb{Q})$, excepto para un número finito de elementos de $\mathbb{Q}$. Por lo tanto las posibilidades de encontrar un $t$ tal que si tenemos $n$ puntos distintos en $E(\mathbb{Q}(T))$ obtengamos $n$ puntos distintos en $\mathcal{E}_t(\overline{\mathbb{Q}})$ será altísima. Es decir que, eligiendo un $t \in \mathbb{Q}$ al azar, con casi toda probabilidad tendremos que $\sigma_t$ es inyectiva.

Por otra parte, el teorema anterior nos dice también

$$rango\, \mathcal{E}_t(\mathbb{Q}) \geq rango\, E(\mathbb{Q}(T))$$

para casi todo $t \in \mathbb{Q}$. Con esto es sensato buscar curvas elípticas $\mathcal{E}_t(\mathbb{Q})$ provenientes de especializar $E(\mathbb{Q}(T))$ para las que el rango de $\mathcal{E}_t(\mathbb{Q})$ sea mayor que el de $E(\mathbb{Q}(T))$.

Nuestro primer objetivo será encontrar curvas elípticas definidas sobre $\mathbb{Q}(T)$ de rango alto para así buscar curvas elípticas, a partir de la anterior, de rango mayor.

## 7.4 La criba $S(N, \mathcal{E})$ para curvas elípticas sobre $\mathbb{Q}(T)$.

Vamos a considerar una aproximación del rango de curvas elípticas definidas sobre $\mathbb{Q}(T)$ análogo al caso de curvas elípticas definidas sobre $\mathbb{Q}$ hecho en la sección anterior. Vamos a asumir que

(i) $\mathcal{E}$ no está definida sobre $\mathbb{Q}$.

(ii) La ecuación de $\mathcal{E}$ está en forma de Weierstrass con coeficientes en $\mathbb{Z}[T]$.

Para un entero $t$, denotamos por $\mathcal{E}_t$ a la curva obtenida de $\mathcal{E}$ por la especialización $\sigma_t : T \mapsto t$ $(t \in \mathbb{Z})$. Como la ecuación de $\mathcal{E}$ está dada en forma de Weierstrass con coeficientes en $\mathbb{Z}[T]$, entonces $\mathcal{E}_t$ con $t \in \mathbb{Z}$ está dada por una ecuación de Weierstrass con coeficientes en $\mathbb{Z}$.

Definimos un análogo de $a_p(E)$ mediante

$$A_p(\mathcal{E}) = \frac{1}{p} \sum_{t=0}^{p-1} a_p(\mathcal{E}_t),$$

donde $a_p(\mathcal{E}_t) = p + 1 - |\mathcal{E}_t(\mathbb{F}_p)|$ si $\mathcal{E}_t$ es una curva elíptica y $a_p(\mathcal{E}_t) = \epsilon_p(\mathcal{E}_t)$ si no. También definimos el análogo de $s_{Nagao}(N, E)$ por

$$S(N, \mathcal{E}) = -\frac{1}{N} \sum_{p \leq N} A_p(\mathcal{E}) \cdot log\, p.$$

Observamos que cuando $\mathcal{E}$ está definido sobre $\mathbb{Q}$, $A_p(\mathcal{E})$ y $S(N, \mathcal{E})$ son iguales a $a_p(E)$ y $s_{Nagao}(N, E)$ respectivamente.

Entonces nos podemos hacer las siguientes preguntas:

(1) ¿Existe $\lim_{N\to\infty} S(N, \mathcal{E})$?

(2) ¿Pueden ser estimadas las diferencias entre $rango\,\mathcal{E}(\mathbb{Q}(T))$, $\limsup_{N\to\infty} S(N, \mathcal{E})$ y $\liminf_{N\to\infty} S(N, \mathcal{E})$ ?

Nagao conjetura lo siguiente:

**Conjetura de Nagao.**

$$rango\,\mathcal{E}(\mathbb{Q}(T)) = \lim_{N\to\infty} S(N, \mathcal{E}).$$

El mismo Nagao ([NA4]) demuestra lo siguiente:

**Teorema 7.4.1** *La conjetura de Nagao es cierta para los siguientes casos:*

- $\mathcal{E}_i : Y^2 = f(X) + T^i$ *donde* $i = 1$ *ó* $2$ *y* $f(X) \in \mathbb{Z}[X]$ *es un polinomio mónico cúbico sin raíces repetidas.*
- $\mathcal{E}_3 : Y^2 = X^3 - 3T^4X - T^2(1 + T^8)$.
- $\mathcal{E}_4 : Y^2 = X^3 - k^2(T^3 - T)^2X$, *donde* $k$ *es un entero no nulo.*
- $\mathcal{E}_5 : Y^2 = X^3 - k^2(T^4 + 1)^2X$, *donde* $k$ *es un entero no nulo.*

*Además, si suponemos cierta la conjetura de Sato-Tate, entonces también se cumple la conjetura de Nagao para*

$$\mathcal{E}_6 : f(T) \cdot Y^2 = f(X),$$

*donde* $f(X) \in Z[X]$ *es un polinomio cúbico y tal que la curva* $y^2 = f(x)$ *es elíptica sin multiplicación compleja.*

De hecho, para demostrar este teorema, Nagao calcula $A_p(\mathcal{E})$, $\lim_{N\to\infty} S(N, \mathcal{E}_i)$ y el rango de $\mathcal{E}_i(\mathbb{Q}(T))$ para $i = 1 \dots 6$. Y obtiene los siguientes rangos:

$$rango\, \mathcal{E}_1(\mathbb{Q}(T)) = 0$$

$$rango\, \mathcal{E}_2(\mathbb{Q}(T)) = \begin{cases} 2 & \text{si } f(X) \text{ factoriza en 3 polinomios.} \\ 1 & \text{si } f(X) \text{ factoriza en 2 polinomios.} \\ 0 & \text{si } f(X) \text{ es irreducible.} \end{cases}$$

$$rango\, \mathcal{E}_3(\mathbb{Q}(T)) = 1$$

$$rango\, \mathcal{E}_4(\mathbb{Q}(T)) = \begin{cases} 1 & \text{si } k \text{ es igual a } \pm \text{ un cuadrado.} \\ 0 & \text{si no.} \end{cases}$$

$$rango\, \mathcal{E}_5(\mathbb{Q}(T)) = \begin{cases} 1 & \text{si } k \text{ es igual a } \pm \text{ un cuadrado.} \\ 0 & \text{si no.} \end{cases}$$

$$rango\, \mathcal{E}_6(\mathbb{Q}(T)) = 1.$$

Recientemente, Silvermann y Rosen ([SIL3],[R-S]) han considerado superficies elípticas $\mathcal{E} \longrightarrow C$ definidas sobre un cuerpo de números $K$ y sobre una curva base $C$ arbitraria. Y demuestran el siguiente teorema:

**Teorema.** *La conjetura de Nagao es cierta para superficies elípticas racionales.*

Una superficie elíptica es racional si es birracionalmente equivalente a $\mathbb{P}^2$. En términos de una ecuación minimal de Weierstrass $Y^2 = X^3 + A(T)X + B(T)$ para $\mathcal{E}$ sobre $K(T)$, una superficie elíptica es racional si y sólo si $grado(A) \leq 3$ y $grado(B) \leq 5$.

## 7.5 Un teorema de Mordell.

En las siguientes secciones vamos a encontrar curvas elípticas de la forma

$$C : y^2 = ax^4 + bx^3 + cx^2 + dx + e,$$

es decir, que el polinomio $ax^4 + bx^3 + cx^2 + dx + e$ no tiene raíces repetidas. El siguiente teorema nos va a permitir poner este tipo de curvas en una forma de Weierstrass.

**Teorema 7.5.1** *Sea $K$ un cuerpo de característica distinta de 2 y sea $C$ una curva eliptica sobre $K$ de la forma*

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e \quad a \neq 0, a, b, c, d, e \in K.$$

*Sea $E$ la curva elíptica dada por*

$$y^2 = x^3 + cx^2 + (bd - 4ae)x + (b^2e + ad^2 - 4ace).$$

*Entonces, $C$ y $E$ son $K(\sqrt{a})$-birracionalmente equivalentes por la aplicación*

$$\phi_{Mordell} : C \longrightarrow E,$$

*dada por*

$$\phi_{Mordell}(x,y) = (-2\sqrt{a}y + 2ax^2 + bx, 4axy + by - 4a\cdot\sqrt{a}x^3 - 3\sqrt{a}bx^2 - 2\sqrt{a}cx - \sqrt{a}d)$$

*Demostración:* Se comprueba observando que la aplicación inversa es

$$\phi^{-1}_{Mordell}(u,v) = \left(x, \frac{2ax^2 + bx - u}{2\sqrt{a}}\right),$$

donde $x = \dfrac{2\sqrt{a}v + 2\,ad + bu}{b^2 - 4\,ac - 4\,au}$.

□

De hecho, se tiene que para $K = \mathbb{Q}$, que es el caso que nos va a interesar, se va a tener que $\phi_{Mordell} : C \longrightarrow E$ es inyectiva y está definida para todo punto $(x,y) \in C(\mathbb{Q})$. El único punto en el que no está definida es en el punto del infinito, $[0,1,0]$. Además, si $a$ es un cuadrado se va a tener que $\phi_{Mordell} : C \longrightarrow E$ está definida sobre $\mathbb{Q}$.

## 7.6 Curvas elípticas de rango alto sobre $\mathbb{Q}(T)$.

### 7.6.1 Mestre: rango $\geq 11$.

Esta sección es un desarrollo detallado del artículo [MES1], en el que Mestre construye una curva elíptica sobre $\mathbb{Q}(t)$, con invariante $j$ no constante y con rango $\geq 11$.

**Lema 7.6.1** *Sea $K$ un cuerpo de característica distinta de 3 y $p(x)$ un polinomio mónico de grado 12 con coeficientes en $K$. Entonces existe una única tripleta $(g, r_1, r_2)$ de elementos de $K[x]$ tales que:*

*(i) $g$ es mónico, grado$(g) \leq 4$, grado$(r_1) \leq 3$ y grado$(r_2) \leq 3$.*

*(ii) $p = g^3 + r_1 g + r_2$.*

*Demostración*: Escribimos $p$ de la siguiente forma:

$$p(x) = x^{12} + \sum_{i=0}^{11} a_i\, x^i.$$

Buscamos $g(x) = \displaystyle\sum_{i=0}^{4} b_i\, x^i \in K[x]$ tal que

$$grado(p - g^3) \leq 7.$$

Mediante un sencillo cálculo obtenemos:

$$b_4 = 1$$
$$b_3 = \frac{a_{11}}{3}$$
$$b_2 = \frac{a_{10}}{3} - \frac{a_{11}^2}{9}$$
$$b_1 = \frac{a_9}{3} + \frac{5\,a_{11}^3}{81} - \frac{2\,a_{11}a_{10}}{9}$$
$$b_0 = \frac{a_8}{3} + \frac{5\,a_{11}^2 a_{10}}{27} - \frac{a_{10}^2}{9} - \frac{2\,a_{11}a_9}{9} - \frac{10\,a_{11}^4}{243}$$

Ahora, $r_1$ y $r_2$ son respectivamente el cociente y el resto de la división de $p - g^3$ por $g$. Y se obtiene $grado(r_1) \leq 3$ y $grado(r_2) \leq 3$.

□

Llamemos $C$ a la curva proyectiva plana de ecuación afín

$$y^3 + r_1(x)y + r_2(x) = 0.$$

Esta curva contiene los puntos

$$P_i = (x_i, g(x_i)), \quad i = 1, \ldots, 12,$$

donde los $x_i$ recorren las raíces de $p(x)$. Si el polinomio $r_1(x)$ es de grado $\leq 2$, entonces $C$ es una curva cúbica.

En esta sección probaremos que si $K = \mathbb{Q}(t)$ se puede elegir $p(x)$ de forma que

(i) Las raíces de $p(x)$ pertenecen a $\mathbb{Q}(t)$.

(ii) El grado de $r_1(x)$ es $\leq 2$.

(iii) $C$ es una cúbica lisa sobre $\mathbb{Q}(t)$ de invariante $j$ no constante.

(iv) Los puntos $P_i$, $i = 1, \ldots, 12$ son linealmente independientes en el grupo asociado a la curva elíptica $C/\mathbb{Q}(T)$.

Así, si elegimos, por ejemplo, $P_{12}$ como origen, se obtiene una curva elíptica sobre $\mathbb{Q}(t)$, donde el grupo de Mordell-Weil es de rango $\geq 11$.

Sean $z_1, \ldots, z_{12}$ indeterminadas, $p = \prod_{i=1}^{12} (x - z_i)$ el polinomio mónico de raíces $z_i$, y $Z = (z_1, \ldots, z_{12})$ el vector de coordenadas $z_i$. Denotamos por

$$S(Z) \;=\; \text{Coeficiente de grado 3 del polinomio } r_1, \text{ obtenido como en el lema 7.6.1 a partir de } p.$$

**Lema 7.6.2** *$S(Z)$ es un polinomio homogéneo de grado 5 en las $z_i$, $i = 1, \ldots, 12$.*

*Demostración:* Tenemos

$$p = \prod_{i=1}^{12} (x - z_i) = \sum_{i=0}^{12} (-1)^i s_{12-i}(Z)\, x^i,$$

donde $s_i(Z)$ son los polinomios simétricos elementales de grado $i$ en las indeterminadas $z_1, \ldots, z_{12}$. Además, cambiando $a_i$ por $s_{12-i}(Z)$ en los coeficientes de $g$ de la demostración del lema 7.6.1, podemos ver que los coeficientes $b_i$ de $g$ son polinomios homogéneos en $Z$ de grado $4 - i$. Así, como grado$(p - g^3) \leq 7$ el coeficiente de $x^7$ en $p - g^3$ es un polinomio homogéneo en $Z$ de grado 5. Al dividir $p - g^3$ por $g$ obtenemos como cociente un polinomio $r_1$ de grado 3, cuyo coeficiente de $x^3$ es un polinomio homogéneo en $Z$ de grado 5, ya que $g$ es mónico.

□

**Lema 7.6.3** *(i) Si $u$ es una indeterminada y $U = (u, \ldots, u)$, entonces*

$$S(Z + U) = S(Z).$$

*(ii) Si $p$ es el cubo de un polinomio, entonces*

$$S(Z) = 0.$$

*(iii) Si $p$ es un polinomio par, entonces*

$$S(Z) = 0.$$

*Demostración*:

(i) Denotamos por $p_u(x)$ al polinomio que tiene como raíces las coordenadas del vector $Z + U$. Se tiene la siguiente identidad

$$p_u(x) = \prod_{i=0}^{12} (x - (z_i + u)) = \prod_{i=0}^{12} (x - u - z_i) = p(x - u). \tag{7.9}$$

Usando el apartado (ii) del lema 7.6.1 obtenemos

$$p(x - u) = g^3(x - u) + g(x - u)r_1(x - u) + r_2(x - u).$$

Y como la descomposición es única,

$$\begin{cases} g_u(x) = g(x - u), \\ r_{1,u}(x) = r_1(x - u), \\ r_{2,u}(x) = r_2(x - u). \end{cases}$$

Por tanto,

$$S(Z + U) = S(Z).$$

(ii) Si $p = g^3$ con $g \in K[x]$, es obvio, ya que $r_1 = 0 = r_2$.

(iii) Si $p(x) = \sum_{i=0}^{12} a_i\, x^i$ es un polinomio par, entonces $a_{2i+1} = 0$ para todo $i$. Y observando cómo son los coeficientes de $g$ vemos que $g$ también es par. Ahora tenemos

$$\begin{aligned} p(x) &= p(-x) \\ g^3(x) + g(x)r_1(x) + r_2(x) &= g^3(-x) + g(-x)r_1(-x) + r_2(-x) \end{aligned}$$

y como $g(x) = g(-x)$,

$$g(x)[r_1(x) - r_1(-x)] + r_2(x) - r_2(-x) = 0.$$

En particular el coeficiente de grado 7 es nulo. Esto es,

$$1 \cdot (S(Z) + S(Z)) = 0.$$

Por tanto, $S(Z) = 0$.

□

**Lema 7.6.4** *Sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ cuatro indeterminadas. El punto*

$$V = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

*es un punto (al menos) doble de la variedad $S$ de ecuación afín $S(Z) = 0$.*

*Demostración*: Por el apartado (ii) del lema 7.6.3, $V$ es un punto de $S$.

Sea $D = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$, y sea $p_\varepsilon$ el polinomio cuyas raíces son las coordenadas del vector $V + \varepsilon D$. Por el lema 7.6.1 tenemos que existen tres polinomios $g_\varepsilon, r_{1,\varepsilon}, r_{2,\varepsilon} \in K[x]$ tales que

$$p_\varepsilon = g_\varepsilon^3 + g_\varepsilon r_{1,\varepsilon} + r_{2,\varepsilon}.$$

Vamos a demostrar que los polinomios $r_{1,\varepsilon}, r_{2,\varepsilon}$ son divisibles por $\varepsilon^2$ en el anillo de polinomios $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \varepsilon][x]$. Por la definición de $p_\varepsilon$ se tiene

$$\begin{aligned} p_\varepsilon(x) &= (x - \alpha_1 + \varepsilon)(x - \alpha_1)^2(x - \alpha_2)^3(x - \alpha_3)^3(x - \alpha_4)^3 = \\ &= \frac{x - \alpha_1}{x - \alpha_1}(x - \alpha_1 + \varepsilon)(x - \alpha_1)^2(x - \alpha_2)^3(x - \alpha_3)^3(x - \alpha_4)^3 = \\ &= \left(1 + \frac{\varepsilon}{x - \alpha_1}\right)(x - \alpha_1)^3(x - \alpha_2)^3(x - \alpha_3)^3(x - \alpha_4)^3. \end{aligned}$$

Ahora hacemos el desarrollo de $\sqrt[3]{1 + s\varepsilon}$ y deducimos

$$\sqrt[3]{1 + \varepsilon s} = 1 + \frac{\varepsilon}{3}s + \varepsilon^2 \sum_{i=2}^{\infty} c_i\, s^i, \qquad c_i \in K.$$

Por lo tanto,

$$g_\varepsilon(x) \equiv (x-\alpha_2)(x-\alpha_3)(x-\alpha_4)\left(x-\alpha_1+\frac{\varepsilon}{3}\right) \bmod \varepsilon^2.$$

Esto es, $p_\varepsilon - g_\varepsilon^3 \equiv 0 \bmod \varepsilon^2$ y así mostramos que los polinomios $r_{1,\varepsilon}, r_{2,\varepsilon}$ son divisibles por $\varepsilon^2$ en $\mathbb{Q}[\alpha_1,\alpha_2,\alpha_3,\alpha_4,\varepsilon][x]$. Por tanto, la aplicación tangente a $S$ en el punto $V$ y en la dirección $D$ es nula; entonces, permutando el papel de $\alpha_1,\alpha_2,\alpha_3,\alpha_4$, la aplicación tangente también es nula. Y obtenemos que $V$ es un punto al menos doble de $S$. Esto prueba el lema.

□

**Lema 7.6.5** *Sean $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ y $T$ cinco indeterminadas. Sean*

$$V = (\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_1,\alpha_2,\alpha_3,\alpha_4),$$
$$W = (\alpha_4,\alpha_4,\alpha_4,\alpha_3,\alpha_3,\alpha_3,\alpha_2,\alpha_2,\alpha_2,\alpha_1,\alpha_1,\alpha_1).$$

*Entonces*

$$S(V+TW) = 0.$$

*Demostración*: Vimos en el lema 7.6.2, que $S(Z)$ era un polinomio homogéneo de grado 5 en las $z_i$, $i = 1,\ldots,12$. Por lo tanto podemos escribir

$$S(V+TW) = \sum_{i=0}^{5} A_i\, T^i,$$

donde $A_i$ es un polinomio homogéneo en $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ de grado $5-i$. El lema 7.6.4 nos asegura que el punto $V$ es un punto doble de $S$, así que

$$A_0 = 0 = A_1.$$

De igual forma que hemos visto que $V$ es un punto doble de $S$, y se comprueba que $W$ también lo es. En consecuencia,

$$S(uV+W) = u^2 \sum_{i=2}^{5} B_i\, u^{i-2}.$$

Por otra parte,

$$S(uV+W) = S\left(u\left(V+\frac{1}{u}W\right)\right) = u^5 S\left(V+\frac{1}{u}W\right) = \sum_{i=2}^{5} A_i\, u^{5-i}.$$

Así que $B_i = A_{5-i}$, y, en particular,

$$A_4 = 0 = A_5.$$

Vemos así que

$$S(V+TW) = T^2 S_1(T),$$

donde $S_1(T)$ es un polinomio de grado $\leq 1$ con respecto a $T$.

Vamos a probar que los puntos

$$V - W \qquad \text{y} \qquad V + W$$

pertenecen a $S$. Con esto tendríamos que $T = 1$ y $T = -1$ serían raíces de $S_1(T)$, que es un polinomio de grado $\leq 1$. Por lo tanto,

$$S_1(T) = 0,$$

y el lema quedaría probado.

$\boxed{T=-1}$ Denotamos por $p_{V-W}$ al polinomio cuyas raíces son las coordenadas de $V-W$, es decir,

$$p_{V-W}(x) = \prod_{\substack{i,j=1 \\ i \neq j}}^{4} (x - (\alpha_i - \alpha_j)) = \prod_{\substack{i,j=1 \\ i < j}}^{4} \left[x^2 - (\alpha_i - \alpha_j)^2\right].$$

Vemos que $p_{V-W}$ es par y por el apartado (iii) del lema 7.6.3,

$$S(V - W) = 0.$$

$\boxed{T=1}$ Análogamente al caso $T = -1$, el polinomio cuyas raíces son las coordenadas del vector $V + W$ es

$$p_{V+W}(x) = \prod_{\substack{i,j=1 \\ i \neq j}}^{4} (x - (\alpha_i + \alpha_j)) = \prod_{\substack{i,j=1 \\ i < j}}^{4} (x - (\alpha_i + \alpha_j))^2.$$

Ahora tomamos $u = -\dfrac{1}{2}(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)$ y $U = (u, \ldots, u)$ para obtener

$$p_{V+W+U}(x) = p_{V+W}(x - u) = \left[x^2 - \tfrac{1}{4}(\alpha_1 + \alpha_3 - (\alpha_2 + \alpha_4))\right]^2 \left[x^2 - \tfrac{1}{4}(\alpha_3 + \alpha_4 - (\alpha_1 + \alpha_2))\right]^2 \left[x^2 - \tfrac{1}{4}(\alpha_1 + \alpha_4 - (\alpha_2 + \alpha_3))\right]^2.$$

Por ser $p_{V+W+U}(x)$ par, el apartado (iii) del lema 7.6.3 nos dice que se tiene $S(V + W + U) = 0$, y el apartado (i) del mismo lema nos asegura que $S(V + W + U) = S(V + W)$. Por tanto, $S(V + W) = 0$.

□

Resumiendo los lemas precedentes,

**Proposición 7.6.6** *Sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ cuatro indeterminadas y*

$$p(T, x) = \prod_{i,j=1; i \neq j}^{4} (x - z_{ij}(T)),$$

*donde $z_{ij}(T) := \alpha_i + T\alpha_j$ con $i, j = 1, \ldots, 4$ e $i \neq j$. Si $g, r_1, r_2$ son los polinomios asociados a $p$ como en el lema* 7.6.1*, el polinomio $r_1$ es de grado $\leq 2$ con respecto a la variable $x$ y la cúbica $C$*

$$y^3 + r_1(T, x)y + r_2(T, x) = 0$$

*contiene los doce puntos $P_{ij} = (z_{ij}(T), g(T, z_{ij}(T)))$, con $i, j = 1, \ldots, 4$ y $i \neq j$.*

*Demostración*: El polinomio $r_1(T, x)$ es de grado $\leq 2$ en la $x$, ya que el coeficiente de grado 3 es $S(V + TW)$ y hemos visto en el lema 7.6.5 que es idénticamente nulo. El resto de las afirmaciones son totalmente obvias por la construcción de $C$.

□

**Observación 7.6.7** Sea $p(T, x) = \prod_{i,j=1;i\neq j}^{12} (x - z_{ij}(T))$, donde $z_{ij}(T) = \alpha_i + T\alpha_j$, como antes, y

$$p(T, x) = g^3(T, x) + g(T, x)r_1(T, x) + r_2(T, x)$$

la descomposición como en el lema 7.6.1. Utilizando la igualdad

$$z_{ij}\left(\frac{1}{T}\right) = \frac{1}{T} z_{ji}(T) \tag{7.10}$$

se tiene que

$$\begin{aligned} p\left(\frac{1}{T}, x\right) &= \prod_{i,j=1;i\neq j}^{12} \left(x - \frac{z_{ji}}{T}\right) = \frac{1}{T^{12}} \prod_{i,j=1;i\neq j}^{12} (Tx - z_{ji}) = \frac{1}{T^{12}} p(T, Tx) = \\ &= \frac{1}{T^{12}} \left[g^3(T, Tx) + g(T, Tx)r_1(T, Tx) + r_2(T, Tx)\right] = \\ &= \left(\frac{g(T, Tx)}{T^4}\right)^3 + \frac{g(T, Tx)}{T^4} \cdot \frac{r_1(T, Tx)}{T^8} + \frac{r_2(T, Tx)}{T^{12}}. \end{aligned}$$

Por otra parte,

$$p\left(\frac{1}{T}, x\right) = g^3\left(\frac{1}{T}, x\right) + g\left(\frac{1}{T}, x\right) r_1\left(\frac{1}{T}, x\right) + r_2\left(\frac{1}{T}, x\right)$$

y como la descomposición es única, por el lema 7.6.1, se tiene

$$\begin{aligned} g\left(\frac{1}{T}, x\right) &= \frac{g(T, Tx)}{T^4}, \\ r_1\left(\frac{1}{T}, x\right) &= \frac{r_1(T, Tx)}{T^8}, \\ r_2\left(\frac{1}{T}, x\right) &= \frac{r_2(T, Tx)}{T^{12}}. \end{aligned} \tag{7.11}$$

**Observación 7.6.8** Podemos ver a $C$ como una superficie elíptica definida sobre el cuerpo $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, fibrada sobre $\mathbb{P}^1$. $C$ posee la siguiente involución

$$((x, y), T) \overset{\phi}{\longmapsto} \left( \left( \frac{x}{T}, \frac{y}{T^4} \right), \frac{1}{T} \right).$$

Para verlo, hemos de probar que

$$\phi : C \longrightarrow C \quad , \quad \phi \neq id_C \quad \text{y} \quad \phi^2 = id_C.$$

Veamos que si $((x, y), T) \in C$, entonces $\left( \left( \frac{x}{T}, \frac{y}{T^4} \right), \frac{1}{T} \right) \in C$. Usando (7.11) se tiene

$$\begin{aligned} &\left( \frac{y}{T^4} \right)^3 + r_1 \left( \frac{1}{T}, \frac{x}{T} \right) \frac{y}{T^4} + r_2 \left( \frac{1}{T}, \frac{x}{T} \right) = \\ &= \frac{y^3}{T^{12}} + \frac{r_1(T, x)}{T^8} \frac{y}{T^4} + \frac{r_2(T, x)}{T^{12}} = \\ &\frac{1}{T^{12}} (y^3 + r_1(T, x) y + r_2(T, x)) = 0 \end{aligned}$$

por pertenecer $((x, y), T)$ a $C$. Ver $\phi \neq id_C$ y $\phi^2 = id_C$ es inmediato.

Enunciamos un lema que nos permite simplificar la ecuación de $C$.

**Lema 7.6.9**

*(i) Los elementos $g(T, z_{ij}(T))$ $i, j = 1, \ldots, 4$ con $i \neq j$, pertenecientes al anillo $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, T]$, donde $z_{ij}(T) = \alpha_i + T\alpha_j$, son divisibles por $T$ y son de grado $\leq 3$ en $T$.*

*(ii) Los polinomios $r_1$ y $r_2$ son divisibles respectivamente por $T^2$ y $T^3$ dentro del anillo $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, T][x]$, y son de grados $\leq 6$ y $\leq 9$ en $T$, respectivamente.*

*Demostración*:

(i) Para $T = 0$, $p$ es el cubo de $p_0 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$, luego

$$g(T, x) = p_0(T, x) + T g_1(T, x)$$

con $g_1 \in \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, T][x]$. Entonces,

$$g(T, z_{ij}(T)) = \prod_{k=1}^{4} (z_{ij}(T) - \alpha_k) + T g_1(T, z_{ij}(T)) \equiv 0 \bmod T$$

por la definición de $z_{ij}(T)$. Denotamos por

$$g(T, z_{ij}(T)) = \sum_{i=0}^{4} C_i T^i \quad \text{y} \quad g\left( \frac{1}{T}, z_{ji}\left( \frac{1}{T} \right) \right) = \sum_{i=0}^{4} D_i T^{-i}.$$

Y utilizando (7.11) y (7.10),

$$\begin{aligned}\sum_{i=0}^{4} C_i\, T^i &= g(T, z_{ij}) = g\left(T, T z_{ji}\left(\frac{1}{T}\right)\right) = \\ &= T^4 g\left(\frac{1}{T}, z_{ji}\left(\frac{1}{T}\right)\right) = \sum_{i=0}^{4} D_i\, T^{4-i} = \sum_{i=0}^{4} D_{4-i}\, T^i.\end{aligned}$$

Luego $D_{4-i} = C_i$, $i = 0, \ldots, 4$. Hemos visto que $g(z_{ij}(T)) \equiv 0 \bmod T$, así que $D_4 = 0 = C_0$; y esto para todo $z_{ij}$, luego el grado de $g(T, z_{ij})$ en $T$ es $\leq 3$.

(ii) Ya vimos en la demostración del lema 7.6.4 que $r_1, r_2$ son divisibles por $T^2$. Tenemos

$$r_2(x) = p(x) - g^3(x) - g(x) r_1(x).$$

Entonces,

$$r_2(z_{ij}) = -g^3(z_{ij}) - g(z_{ij}) r_1(z_{ij}),$$

por lo que $T^3$ divide a $r_2(z_{ij})$ para todo $i, j$. El polinomio $\dfrac{r_2(x)}{T^2}$ es de grado $\leq 3$ en $x$, ya que $r_2(x)$ también lo es por el lema 7.6.1. Por definición tenemos $z_{ij}(0) = \alpha_i$ y por el apartado (ii) del lema 7.6.3 obtenemos

$$\frac{r_2(\alpha_i)}{T^2} = 0 \qquad i = 1, \ldots, 4,$$

es decir, $\dfrac{r_2(x)}{T^2} \equiv 0 \bmod T$, esto es, $r_2$ es divisible por $T^3$.

Se tiene por construcción que el grado de $r_1$ en $T$ es $\leq 8$ y el de $r_2$ es $\leq 12$. Además, como vimos en la proposición 7.6.6, se tiene que el grado de $r_1$ en $x$ es $\leq 2$ y el de $r_2$ es $\leq 3$. Por tanto podemos escribir

$$\begin{aligned} r_1(T, x) &= \sum_{i=0}^{2} A_i(T)\, x^i \quad \text{con grado}(A_i(T)) \leq 8; \\ r_2(T, x) &= \sum_{i=0}^{3} B_i(T)\, x^i \quad \text{con grado}(B_i(T)) \leq 12. \end{aligned}$$

Utilizando las identidades (7.11) obtenemos

$$\sum_{i=0}^{2} A_i\left(\frac{1}{T}\right) x^i = r_1\left(\frac{1}{T}, x\right) = \frac{r_1(T, Tx)}{T^8} = \sum_{i=0}^{2} \frac{A_i(T)}{T^{8-i}}\, x^i,$$

y con ello que

$$A_i(T) = T^{8-i} A_i\left(\frac{1}{T}\right).$$

Si denotamos $A_i(T) = \sum_{k=0}^{8} a_{i,k}\, T^k$, obtenemos

$$\begin{aligned} i=0 &\implies \quad a_{0,k} = a_{0,8-k} \quad k=0,\dots,8; \\ i=1 &\implies \begin{cases} a_{1,8}=0, \\ a_{1,k} = a_{1,7-k} \quad k=0,\dots,7; \end{cases} \\ i=2 &\implies \begin{cases} a_{2,8} = a_{2,7} = 0, \\ a_{2,k} = a_{2,6-k} \quad k=0,\dots,6; \end{cases} \end{aligned} \tag{7.12}$$

Hemos visto que $T^2 \,|\, r_1$, por lo que $a_{i,0} = a_{i,1} = 0$, $i = 0,1,2$. Con (7.12) obtenemos $a_{i,8} = a_{i,7} = 0$, $i = 0,1,2$, es decir que el grado en $T$ de $r_1$ es $\leq 6$.

Para $r_2$, utilizando de nuevo las identidades (7.11) obtenemos

$$\sum_{i=0}^{3} B_i\left(\frac{1}{T}\right) x^i = r_2\left(\frac{1}{T}, x\right) = \frac{r_2(T,Tx)}{T^{12}} = \sum_{i=0}^{3} \frac{B_i(T)}{T^{12-i}}\, x^i.$$

Así que

$$B_i(T) = T^{12-i} B_i\left(\frac{1}{T}\right).$$

Si denotamos $B_i(T) = \sum_{k=0}^{12} b_{i,k}\, T^k$, obtenemos

$$\begin{aligned} i=0 &\implies \quad b_{0,k} = b_{0,12-k} \quad k=0,\dots,12; \\ i=1 &\implies \begin{cases} b_{1,12}=0, \\ b_{1,k} = b_{1,11-k} \quad k=0,\dots,11; \end{cases} \\ i=2 &\implies \begin{cases} b_{2,12} = b_{2,11} = 0, \\ b_{2,k} = b_{2,10-k} \quad k=0,\dots,10; \end{cases} \\ i=3 &\implies \begin{cases} b_{3,12} = b_{3,11} = b_{3,10} = 0, \\ b_{3,k} = b_{3,9-k} \quad k=0,\dots,9. \end{cases} \end{aligned} \tag{7.13}$$

Como $T^3 \,|\, r_2$, $b_{i,0} = b_{i,1} = b_{i,2} = 0$, $i = 0,1,2,3$. Junto con (7.13) obtenemos $b_{i,12} = b_{i,11} = b_{i,10} = 0$, $i = 0,1,2,3$; es decir, que el grado en $T$ de $r_2$ es $\leq 9$.

□

Cambiando $y$ por $Y = Ty$, la ecuación de $C$ queda de la forma

$$Y^3 + f_1(T,x)Y + f_2(T,x) = 0,$$

donde $f_1$ (respectivamente $f_2$) es de grado $\leq 2$ en $x$ y $\leq 4$ en $T$ (respectivamente $\leq 3$ en $x$ y $\leq 6$ en $T$).

Los puntos $P_{ij} = \left(z_{ij}(T), \dfrac{g(z_{ij}(T))}{T}\right)$ tienen coodenadas sobre $\mathbb{Q}[\alpha_1,\dots,\alpha_4,T]$ $z_{ij}(T)$ (respectivamente $\dfrac{g(z_{ij}(T))}{T}$) de grado $\leq 1$ (respectivamente $\leq 2$) en $T$.

Nos falta por mostrar que para $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ convenientemente elegidos, $C$ es lisa, los puntos $P_{ij}$ son linealmente independientes y el invariante $j$ de $C$ es no constante. Eligiendo

$$\boxed{\alpha_1 = -1 \ , \ \alpha_2 = 0 \ , \ \alpha_3 = 2 \text{ y } \alpha_4 = 11}$$

obtenemos la siguiente curva

$$E : y^3 + a_1x^2y + a_2xy + a_3y + a_4x^3 + a_5x^2 + a_6x + a_7 = 0,$$

con

$$\begin{aligned}
a_1 &= -26940T^2 + 51220T - 26940,\\
a_2 &= -1320T^3 + 17280T^2 + 17280T - 1320,\\
a_3 &= -18876T^4 - 153828T^3 + 301221T^2 - 153828T - 18876,\\
a_4 &= -1489600T^3 + 1489600T^2 + 1489600T - 1489600,\\
a_5 &= 5816880T^4 + 8043880T^3 - 27463500T^2 + 8043880T + 5816880,\\
a_6 &= 3416160T^5 - 24166320T^4 + 19202040T^3 + 19202040T^2\\
&\quad - 24166320T + 3416160\\
a_7 &= -745360T^6 - 15468024T^5 + 18853764T^4\\
&\quad - 138394T^3 + 18853764T^2 - 15468024T - 745360.
\end{aligned}$$

Los puntos $P_{ij}$ con $i, j = 1, \ldots, 4$, $i \neq j$, los denotaremos por $P_k$ con $k = 1, \ldots, 12$. Así, los puntos $P_k$ tienen como coordenadas:

$$\begin{aligned}
P_1 &= (11T - 1, -1584T^2 + 1826T - 240),\\
P_2 &= (11T, -396T^2 + 73T + 154),\\
P_3 &= (11T + 2, 1980T^2 - 1399T - 414),\\
P_4 &= (2T + 11, -414T^2 - 1399T + 1980)\\
P_5 &= (2T - 1, 234T^2 - 487T + 84),\\
P_6 &= (2T, 180T^2 - 134T - 44),\\
P_7 &= (2, -44T^2 - 134T + 180),\\
P_8 &= (11, 154T^2 + 73T - 396),\\
P_9 &= (-1, -110T^2 + 121T + 156),\\
P_{10} &= (-T, 156T^2 + 121T - 110),\\
P_{11} &= (-T + 2, 84T^2 - 487T + 234),\\
P_{12} &= (-T + 11, -240T^2 + 1826T - 1584).
\end{aligned}$$

Vamos a ver que los doce puntos anteriores son independientes. Primero veremos la demostración realizada por Mestre en [MES1].

Para mostrar que los puntos $P_k$ son independientes, es cómodo ver $E$ como una superficie elíptica fibrada sobre $\mathbb{P}^1$ y los puntos $P_k$ como secciones de la fibración $E \longrightarrow \mathbb{P}^1$ dada por $(x, y, T) \longmapsto T$.

El discriminante es un polinomio en $T$ irreducible de grado 36. Las fibras singulares son de tipo Kodaira $I_1$, es decir, son cúbicas nodales. Si elegimos el punto $P_{12}$ como elemento neutro $\mathcal{O}$, la forma bilineal de Néron-Tate viene dada, después de Shioda ([SHI]), por

$$\langle P, Q \rangle = \chi + (P \cdot \mathcal{O}) + (Q \cdot \mathcal{O}) - (P \cdot Q),$$

donde $(R \cdot S)$ designa el producto de intersección de las secciones $R$ y $S$, y $\chi_{\mathcal{E}}$ es la característica de Euler-Poincaré de la superficie $\mathcal{E}$.

Ahora vamos a calcular $\chi_{\mathcal{E}}$ usando la siguiente fórmula:

**Fórmula de Noether.** *Sea $\mathcal{S}$ una superficie compleja y conexa. Entonces*

$$\chi_{\mathcal{S}} = \frac{K_{\mathcal{S}}^2 + \chi_{top}(\mathcal{S})}{12},$$

*donde $K_{\mathcal{S}}$ es el divisor canónico de $\mathcal{S}$ y $\chi_{top}(\mathcal{S})$ es la característica topológica de $\mathcal{S}$.*

Para superficies elípticas $\mathcal{E}$ se tiene que (ver [BEA], Capítulo IX, Proposición IX.3)

$$K_{\mathcal{E}}^2 = 0. \tag{7.14}$$

Por lo tanto sólo nos queda calcular $\chi_{top}(\mathcal{E})$ y para ello enunciaremos el siguiente resultado que se puede encontrar en [B-P-V], Capítulo III, Sección 11, Proposición 11.4.

**Proposición 7.6.10** *Sea $\pi : \mathcal{S} \longrightarrow C$ una fibración sobre la curva $C$ de la superficie compacta $\mathcal{S}$ y sea $\mathcal{S}_{gen}$ una fibra genérica. Entonces, si $\mathcal{S}_t = \pi^{-1}(t)$,*

$$\chi_{top}(\mathcal{S}) = \chi_{top}(\mathcal{S}_{gen}) \cdot \chi_{top}(C) + \sum_{t \in C} (\chi_{top}(\mathcal{S}_t) - \chi_{top}(\mathcal{S}_{gen})).$$

Vamos a aplicar esta proposición a nuestra superficie elíptica $\mathcal{E}$. En este caso, la fibra genérica es una curva elíptica y por tanto $\chi_{top}(\mathcal{E}_{gen}) = 0$. Si $\mathcal{E}_t$ es una fibra singular entonces $\chi_{top}(\mathcal{E}_t) = 1$, por ser cúbicas nodales. Hay 36 fibras singulares, ya que el discriminante es un polinomio de grado 36, y por tanto,

$$\chi_{top}(\mathcal{E}) = 36. \tag{7.15}$$

Por tanto usando (7.14) y (7.15) en la fórmula de Noether, obtenemos

$$\chi_{\mathcal{E}} = 3.$$

Los lemas siguientes nos permiten calcular $(P_i \cdot P_j)$, $1 \leq i, j \leq 12$.

**Lema 7.6.11** *Sean $i, j$ dos índices distintos ($1 \leq i, j \leq 12$). Denotamos por*

$$x_i = a_i + Tb_i \qquad y \qquad x_j = a_j + Tb_j$$

*las abcisas de $P_i$ y $P_j$. Entonces*

$$(P_i \cdot P_j) = \begin{cases} 0 & \text{si } (a_i - a_j)(b_i - b_j) = 0, \\ 1 & \text{en otro caso} \end{cases}$$

*Demostración*: Primero, hemos de tener que las abcisas coinciden:

$$\begin{aligned} a_i + Tb_i &= a_j + Tb_j, \\ (a_i - a_j) &= (b_j - b_i)T. \end{aligned}$$

Se van a distinguir varios casos:

- Si $a_i = a_j$, entonces
$$b_i = b_j \qquad \text{ó} \qquad T = 0.$$
Si $b_i = b_j$, se tiene que $P_i = P_j$, y entonces $i = j$.
Si $T = 0$ y denotamos por $h_i(T)$ a la ordenada del punto $P_i$, como se tiene que $h_i(0) \neq h_j(0)$ si $i \neq j$, entonces
$$(P_i \cdot P_j) = 0.$$

- Si $b_i = b_j$, entonces $a_i = a_j$ y por tanto $P_i = P_j$ y hemos supuesto que $i \neq j$.

- Si $(a_i - a_j)(b_i - b_j) \neq 0$, obtenemos $T = \dfrac{a_i - a_j}{b_j - b_i}$. Ahora, se observa que
$$p_i\left(\frac{a_i - a_j}{b_j - b_i}\right) = p_j\left(\frac{a_i - a_j}{b_j - b_i}\right) \quad \forall i, j \text{ tal que } i \neq j;$$
por tanto, $(P_i \cdot P_j) = 1$.

□

Y para la autointersección tenemos el siguiente resultado:

**Lema 7.6.12** *Para cualquier sección $P \in \mathcal{E}(\mathbb{P}^1)$ se tiene que*

$$(P^2) = (\mathcal{O}^2) = -\chi_{\mathcal{E}}.$$

*Demostración:* Ver [SHI] Lema 2.7.

Así, la matriz de alturas de los puntos $P_i$, $i = 1, \ldots, 11$ es:

$$\begin{pmatrix} 8 & 5 & 5 & 3 & 5 & 4 & 4 & 3 & 5 & 3 & 3 \\ 5 & 8 & 5 & 3 & 4 & 5 & 4 & 3 & 4 & 4 & 3 \\ 5 & 5 & 8 & 3 & 4 & 4 & 5 & 3 & 4 & 3 & 4 \\ 3 & 3 & 3 & 6 & 4 & 4 & 3 & 3 & 3 & 2 & 2 \\ 5 & 4 & 4 & 4 & 8 & 5 & 4 & 3 & 5 & 3 & 3 \\ 4 & 5 & 4 & 4 & 5 & 8 & 4 & 3 & 4 & 4 & 3 \\ 4 & 4 & 5 & 3 & 4 & 4 & 8 & 4 & 5 & 3 & 4 \\ 3 & 3 & 3 & 3 & 3 & 3 & 4 & 6 & 4 & 2 & 2 \\ 5 & 4 & 4 & 3 & 5 & 4 & 5 & 4 & 8 & 3 & 3 \\ 3 & 4 & 3 & 2 & 3 & 4 & 3 & 2 & 3 & 6 & 3 \\ 3 & 3 & 4 & 2 & 3 & 3 & 4 & 2 & 3 & 3 & 6 \end{pmatrix}$$

con determinante igual a $2^{16}3^4$, que no es nulo; esto prueba la independencia de los puntos $P_i$, $i = 1, \ldots, 11$.

Ahora vamos a ver una segunda demostración que utiliza los teoremas de especialización que vimos en la sección 7.3. El teorema 7.3.3 nos asegura que la aplicación especialización $\sigma_t$ es inyectiva para todo $t \in \mathbb{Q}$, excepto para un número finito, comenzamos a ver $\sigma_1, \sigma_2, \ldots$ pero obtenemos que no son inyectivas, hasta llegar a $t = 5$, con la que conseguimos mandar los doce puntos a otros doce puntos distintos, que es lo que necesitamos. Así, mediante $\sigma_5 : t \longrightarrow 5$, obtenemos que los coeficientes de la curva pasan a

$(a_1)_5 = -444340,$
$(a_2)_5 = 352080,$
$(a_3)_5 = -24283491,$
$(a_4)_5 = -143001600,$
$(a_5)_5 = 4000483780,$
$(a_6)_5 = -1665559440,$
$(a_7)_5 = -47824263130,$

y los puntos $P_k$

$(P_1)_5 = (54, -30710),$
$(P_2)_5 = (55, -9381),$
$(P_3)_5 = (57, 42091),$
$(P_4)_5 = (21, -15365)$
$(P_5)_5 = (9, 3499),$
$(P_6)_5 = (10, 3786),$
$(P_7)_5 = (2, -1590),$
$(P_8)_5 = (11, 3819),$
$(P_9)_5 = (-1, -1989),$
$(P_{10})_5 = (-5, 4395),$
$(P_{11})_5 = (-3, -101),$
$(P_{12})_5 = (6, 1546).$

Elegimos el punto $(P_{12})_5$ como elemento neutro y pasamos esta ecuación a la siguiente forma de Weierstrass, que en el lenguaje del sistema de cálculo PARI es

```
E=initell([0,0,0,-40882674303743037258350100,
             10055650355690605483027446611428399000]);
```

Y los puntos $(P_1)_5, \ldots, (P_{11})_5$ pasan a

```
p1=[3865711467558825/1024,-4716889734942144411925/32768];
p2=[192889611336410/49,-2705385731255451387 00/343];
p3=[-2086675407042006/289,-215972211151055631173 72/4913];
p4=[3763450258650, -20924283887279500];
p5=[18254953880490, -73739995889820064700];
p6=[624198567198449/64,-12846691864117539671607/512];
p7=[790409610736625/64,19692846711370067937975/512];
```

```
p8=[6967759898090, -12408801087627044100];
p9=[3445873909274, -772289830512462132];
p10=[433705933180250/121,3492887565645307555700/1331];
p11=[32422531814410/9, -4671078429048768100/27];
```

Usando el sistema de cálculo PARI tenemos que el determinante de la matriz

$$(< pi, pj >)_{1\leq i,j\leq 11}$$

asociado a la altura canónica es, en el lenguaje de PARI:

```
m=mathell(E,[p1,p2,p3,p4,p5,p6,p7,p8,p9,p10,p11]);
det(m)=31803732646.56403528873158196.
```

Por lo tanto vemos que $p1, \ldots, p11$ son puntos independientes, ya que el determinante anterior es no nulo. La proposición 7.3.2 nos dice que entonces los puntos $P_1, \ldots, P_{11}$ son independientes.

□

Como hemos afirmado antes, el discriminante es un polinomio en $T$ irreducible de grado 36. Por lo tanto tenemos que su invariante $j$ es no constante y hemos demostrado el siguiente teorema:

**Teorema 7.6.13** *Existe una familia infinita de curvas elípticas, no isomorfas entre sí, definidas sobre* $\mathbb{Q}$ *de rango* $\geq 11$.

### 7.6.2 Mestre: rango $\geq 12$.

En esta sección vamos a describir un segundo método debido a Mestre ([MES1] y [MES2]), con el que obtendremos curvas elípticas definidas sobre $\mathbb{Q}(T)$ con rango $\geq 12$. En la práctica este método resulta más efectivo que el método descrito en la anterior sección.

Sean $\alpha_i \in \mathbb{Z}$, $i = 1, \ldots, 6$, y definamos

$$q(x) = \prod_{i=1}^{6} (X - \alpha_i) \in \mathbb{Q}[X]$$

y

$$p(x) = q(x - T) \cdot q(x + T) \in \mathbb{Q}(T)[X].$$

Entonces existen dos polinomios $g(X), r(X) \in \mathbb{Q}(T)[X]$ con grados 6 y 5 respectivamente tales que

$$p = g^2 - r.$$

Si $p = \sum_{i=0}^{11} a_i\, x^i + x^{12}$, entonces $g = \sum_{i=0}^{6} b_i\, x^i$ con

$$
\begin{aligned}
b_6 &= 1,\\
b_5 &= \frac{a_{11}}{2},\\
b_4 &= \frac{a_{10}}{2} - \frac{{a_{11}}^2}{8},\\
b_3 &= \frac{a_9}{2} - \frac{a_{11}a_{10}}{4} + \frac{{a_{11}}^3}{16},\\
b_2 &= \frac{a_8}{2} - \frac{{a_{10}}^2}{8} + \frac{3\,a_{10}{a_{11}}^2}{16} - \frac{5\,{a_{11}}^4}{128} - \frac{a_{11}a_9}{4},\\
b_1 &= -\frac{a_{11}a_8}{4} + \frac{3\,a_{11}{a_{10}}^2}{16} - \frac{5\,a_{10}{a_{11}}^3}{32} + \frac{7\,{a_{11}}^5}{256} + \frac{3\,{a_{11}}^2a_9}{16} + \frac{a_7}{2} - \frac{a_{10}a_9}{4},\\
b_0 &= \frac{3\,{a_{11}}^2a_8}{16} - \frac{15\,{a_{11}}^2{a_{10}}^2}{64} + \frac{35\,{a_{11}}^4a_{10}}{256} - \frac{21\,{a_{11}}^6}{1024} - \frac{5\,a_9{a_{11}}^3}{32} - \frac{a_{11}a_7}{4}\\
&\quad + \frac{3\,a_9a_{11}a_{10}}{8} - \frac{a_{10}a_8}{4} + \frac{{a_{10}}^3}{16} + \frac{a_6}{2} - \frac{{a_9}^2}{8}.
\end{aligned}
$$

Se observa que la curva $Y^2 = r(X)$ contiene 12 puntos $\mathbb{Q}(T)$-racionales dados por

$$P_i = (T + \alpha_i, g(T + \alpha_i)) \qquad i = 1, \ldots, 6$$

y

$$P_{6+i} = (-T + \alpha_i, g(-T + \alpha_i)) \qquad i = 1, \ldots, 6.$$

Sea $C_5$ el coeficiente de $X^5$ en $r(X)$. Para cualquier 6-upla

$$A = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) \in \mathbb{A}^6(\mathbb{Z})$$

tal que $C_5 = 0$, obtenemos una curva elíptica

$$\mathcal{E}_A : Y^2 = r(X)$$

sobre $\mathbb{Q}(T)$. Para $t \in \mathbb{Q}$, denotamos por $\mathcal{E}_{A,t}$ a la curva elíptica obtenida de $\mathcal{E}_A$ por la especialización $T \longrightarrow t$.

Ahora, tomemos $A = (-17, -16, 10, 11, 14, 17)$. Entonces obtenemos $C_5 = 0$. Y el coeficiente de $X^4$ es de la forma $34749/4T^2 + 4314060$. Para $T = 6$ esta expresión es igual a $2151^2$ y la cónica $U^2 = 34749/4T^2 + 4314060$ es $\mathbb{Q}$-isomorfa a la recta proyectiva. Y podemos parametrizarla por

$$\begin{cases} T = \dfrac{6T'^2 - 956T' + 2574}{T'^2 - 429}, \\ U = -\dfrac{8305011 + 19359T'^2 - 208494T'}{T'^2 - 429}. \end{cases}$$

Con esto Mestre ([MES2]) obtiene el siguiente resultado:

**Teorema 7.6.14** *Sea $A = (-17, -16, 10, 11, 14, 17)$. Entonces,*

$$rango\, \mathcal{E}_A(\mathbb{Q}(T')) \geq 12.$$

*Además su invariante $j$ es no constante.*

*Demostración:* La curva elíptica $\mathcal{E}_A$ está dada por

$$\begin{aligned} Y^2 = & \left(4314060 + \frac{34749}{4}T^2\right)X^4 + \left(-\frac{220077}{2}T^2 - 100359000\right)X^3 \\ & + \left(-\frac{34749}{2}T^4 - \frac{198531}{4}T^2 + 98994636\right)X^2 \\ & + \left(\frac{220077}{2}T^4 - 73669176T^2 + 10917208512\right)X \\ & + \frac{34749}{4}T^6 - 5442147T^4 + 1077301944T^2 - 61466790384, \end{aligned}$$

y los puntos por

$$\begin{aligned} P_1 &= (T - 17, -796824 - \tfrac{7101}{2}T^2 + 103059T), \\ P_2 &= (T - 16, 694980 + \tfrac{6705}{2}T^2 - 100728T), \\ P_3 &= (T + 10, -19656 + \tfrac{621}{2}T^2 - 1161T), \\ P_4 &= (T + 11, 13608 - \tfrac{1557}{2}T^2 - 13491T), \\ P_5 &= (T + 14, -33480 - \tfrac{3195}{2}T^2 - 30303T), \\ P_6 &= (T + 17, 141372 + \tfrac{4527}{2}T^2 + 42624T), \\ P_7 &= (-T - 17, 796824 + \tfrac{7101}{2}T^2 + 103059T), \\ P_8 &= (-T - 16, -694980 - \tfrac{6705}{2}T^2 - 100728T), \\ P_9 &= (-T + 10, 19656 - \tfrac{621}{2}T^2 - 1161T), \\ P_{10} &= (-T + 11, -13608 + \tfrac{1557}{2}T^2 - 13491T), \\ P_{11} &= (-T + 14, 33480 + \tfrac{3195}{2}T^2 - 30303T), \\ P_{12} &= (-T + 17, -141372 - \tfrac{4527}{2}T^2 + 42624T). \end{aligned}$$

Utilizamos la especialización $\sigma_6 : T \longrightarrow 6$ para obtener:

$$Y^2 = 4626801X^4 - 104320386X^3 + 74690505X^2 + 8407728072X - 29331630576,$$

y los puntos $P_i$ pasan a

$$\begin{aligned} (P_1)_6 &= (-11, -306288), \\ (P_2)_6 &= (-10, 211302), \\ (P_3)_6 &= (16, -15444), \\ (P_4)_6 &= (17, -95364), \\ (P_5)_6 &= (20, -272808), \\ (P_6)_6 &= (23, 478602), \\ (P_7)_6 &= (-23, 1542996), \\ (P_8)_6 &= (-22, -1420038), \\ (P_9)_6 &= (4, 1512), \\ (P_{10})_6 &= (5, -66528), \\ (P_{11})_6 &= (8, -90828), \\ (P_{12})_6 &= (11, 32886). \end{aligned}$$

con $(P_i)_6 \in \mathcal{E}_{A,6}(\mathbb{Q})$ $i = 1, \ldots 12$. Ahora mediante la aplicación $\phi_{Mordell}$ obtenemos la curva $E$ y la imagen de los puntos, que en el lenguaje del sistema de cálculo PARI es

```
E=initell([0,74690505,0,-334250967131406288,
                          484049415152194177692862 08]);
p1=[3584861064,214195929837120];
p2=[1059542856,31105904933376];
p3=[766236024,-16911907412400];
p4=[1311100344,-44635421310480];
p5=[2788653096,-146230410534624];
p6=[436840776,77033908224];
p7=[656555544,12006886666320];
p8=[12882795336,1465008463885824];
p9=[-275728536,-11193002664480];
p10=[-4058424,-7054263748224];
p11=[148409496,-1926859079376];
p12=[-169313976,10113639782400];
```

Usando el sistema de cálculo PARI tenemos que el determinante de la matriz

$$(< pi, pj >)_{1\leq i,j\leq 12}$$

asociado a la altura canónica es

```
m=det(mathell(E,[p1,p2,p3,p4,p5,p6,p7,p8,p9,p10,p11,p12]))
m=7.297272887272600092779928942
```

Por lo tanto vemos que $p1, \ldots, p12$ son puntos independientes, ya que el determinante anterior es no nulo. Como la especialización $\sigma_6$ es un homomorfismo de grupos obtenemos que los puntos $P_1, \ldots, P_{12}$ son independientes.

Para ver que el invariante $j$ es no constante hemos de ver que el discriminante es no constante. El discriminante es

$$\begin{aligned}
&28304130721767865217723664991026885306581652602880 00 + \\
&33306747191272951815287986554584780187731144736768 0\,T^2 - \\
&13915315777109032017765256144027745567082357274705 92\,T^4 + \\
&11137293577138163662213175185487780710852140982272 0\,T^6 - \\
&17814010572676902005458960539953063808097506547 20\,T^8 - \\
&29331748914845184131747184124429996585697184\,T^{12} + \\
&11349970098876539536025750827151900909167292160\,T^{10} + \\
&17491335488113481771018062394419981106 40\,T^{14} + \\
&12603240333979283641720918251528756872 1\,T^{16} - \\
&18321575529365466194362553628014700 0\,T^{18} + \\
&54337280303407689533958102090000\,T^{20}.
\end{aligned}$$

□

### 7.6.3 Nagao: rango $\geq 13$.

Vamos a encontrar una curva elíptica sobre $\mathbb{Q}(T)$ de rango $\geq 13$ utilizando el método desarrollado en la sección §7.6.2. Para obtener curvas elípticas $\mathcal{E}_A$ de rango

alto sobre $\mathbb{Q}(T)$, debemos de encontrar 6-uplas $A \in \mathbb{A}^6(\mathbb{Z})$ satisfaciendo $C_5 = 0$ y tales que $S(N, \mathcal{E}_A)$ sea grande.

Para $A = (148, 116, 104, 57, 250)$, tenemos que $C_5 = 0$. Para el valor de $S(N, \mathcal{E}_A)$, tomamos una cierta ecuación de Weierstrass de $\mathcal{E}_A$ con coeficientes en $\mathbb{Z}$, que denotaremos por $\mathcal{E}_{Wei,A}$. Para la curva $\mathcal{E}_{Wei,A}$ tenemos $S(536, \mathcal{E}_{Wei,A}) \geq 10$. En este caso, la ecuación de la curva asociada a $\mathcal{E}_A$ y sus puntos $\mathbb{Q}(T)$)-racionales $P_1, \ldots, P_{12}$ están dados por:

$$\begin{aligned} Y^2 = {} & (9T^2 + 211950)X^4 + (-2700T^2 - 63901710)X^3 + (-18T^4 + 396150T^2 \\ & + 6706476489)X^2 + (2700T^4 - 29575350T^2 - 284435346600)X \\ & + 9T^6 - 159200T^4 + 891699592T^2 + 4156297690000, \end{aligned}$$

$$\begin{aligned} P_1 &= (T + 148, 662T^2 + 66873T + 1868944), \\ P_2 &= (T + 116, -554T^2 - 39687T - 191632), \\ P_3 &= (T + 104, -526T^2 - 28497T + 163372), \\ P_4 &= (T + 57, 508T^2 - 19332T - 368809), \\ P_5 &= (T + 25, 580T^2 - 49116T + 566825), \\ P_6 &= (T, -670T^2 + 69759T - 2038700), \\ P_7 &= (-T + 148, -662T^2 + 66873T - 1868944), \\ P_8 &= (-T + 116, 554T^2 - 39687T + 191632), \\ P_9 &= (-T + 104, 526T^2 - 28497T - 163372), \\ P_{10} &= (-T + 57, -508T^2 - 19332T + 368809), \\ P_{11} &= (-T + 25, -580T^2 - 49116T - 566825), \\ P_{12} &= (-T, 670T^2 + 69759T + 2038700). \end{aligned}$$

Mediante una búsqueda exhaustiva, obtenemos otro punto $\mathbb{Q}(T)$-racional de $\mathcal{E}_A$:

$P_{13} = ((T + 703)/15, (-224T^3 - 844T^2 + 900484T + 2161725)/75)$.

Sea $C_4(T) = 9T^2 + 211950$ el coeficiente de $X^4$ en $r$. Entonces la ecuación

$$S^2 = C_4(T)$$

tiene la siguiente solución parametrizada por

$$(T, S) = \left( \frac{-T'^2 + 23550}{2T'}, \frac{3(T'^2 + 23550)}{2T'} \right).$$

Ahora consideramos la curva $\mathcal{E}'_A$, definida sobre el cuerpo de funciones $\mathbb{Q}(T')$ que se obtiene de $\mathcal{E}_A$ mediante el cambio

$$T \longrightarrow \frac{-T'^2 + 23550}{2T'}.$$

Así Nagao ([NA3]) obtiene:

**Teorema 7.6.15** *Sea* $A = (148, 116, 104, 57, 250)$. *Entonces*

$$rango\, \mathcal{E}'_A(\mathbb{Q}(T')) \geq 13.$$

*Además su invariante* $j$ *es no constante.*

*Demostración:* Análoga a la demostración del teorema 7.6.14, pero en este caso la especialización es

$$\sigma_1 : T \longrightarrow 1.$$

Y al especializar la ecuación de $E$ y sus puntos racionales $p_i$ $(i = 1, 2, .., 13)$ obtenemos

$$\begin{aligned}
Y^2 = 9(&23551^2X^4 - 332790042120X^3 - 614965734912980666X^2 \\
&+ 1845044358377888346 00X + 17052160251222432338 1326809) \\
p_1 &= (23845, 740545471584), \\
p_2 &= (23781, -618187274016), \\
p_3 &= (23757, -586075278288), \\
p_4 &= (23663, 561604339872), \\
p_5 &= (23599, 638662269024), \\
p_6 &= (23549, -736549528176), \\
p_7 &= (-23253, -727947133368), \\
p_8 &= (-23317, 610710560712), \\
p_9 &= (-23341, 580706671464), \\
p_{10} &= (-23435, -565246334016), \\
p_{11} &= (-23499, -647915330496), \\
p_{12} &= (-23549, 749691565704), \\
p_{13} &= (4991/3, -117044707247104/3).
\end{aligned}$$

Cambiando las coordenadas $(X, Y)$ a

$$\begin{aligned}
&((1663948803X^2 - 499185063180X - 23551Y - 307482867456490335)/24, \\
&(-39187658259453X^3 + 17634459470479467X^2 + 554649601XY + \\
&217245870349025965606 29X - 83197486979Y - \\
&325894766882895617625 8115)/48),
\end{aligned}$$

conseguimos la ecuación de Weierstrass de $E$ y los puntos pasan a, en el lenguaje de PARI:

```
E=initell([1,0,0,-19704738598664239380275632932022 11,
33666977357380599346718366106269137257495662819841]);
p1=[25386174421432494,671095236064143178962 33];
p2=[26509492766907566,-24565398404029518279 7783];
p3=[26399379919965810,-21479485931015632557 7539];
p4=[24966084178226490,18290752521007926558 7329];
p5=[24682088239127826,26082767893197990747 3297];
p6=[25869170713328826,-66811158987551134918 203];
p7=[25873709433784550,68073651220906477508 921];
p8=[24768067209581670,-23726856187488750923 2071];
p9=[24875645484381876,-20775310317436214871 0903];
p10=[26306960164950894,18892767630147965622 6153];
p11=[26597669117443566,27039662839354335705 3417];
p12=[25390343800982316,-65957033567927528804 583];
p13=[230674528980533950/9,-18302756499094107331 33/27];
```

El determinante de la matriz

$$(< pi, pj >)_{1\leq i,j\leq 13}$$

asociado a la altura canónica es

```
m=det(mathell(E,[p1,p2,p3,p4,p5,p6,p7,p8,p9,p10,p11,p12,p13]))
m=2910704763254221.2813489
```

Por lo tanto vemos que $p1, \ldots, p13$ son puntos independientes, ya que el determinante anterior es no nulo. Como la especialización $\sigma_1$ es un homomorfismo de grupos obtenemos que los puntos $P_1, \ldots, P_{13}$ son independientes.

Veamos que su invariante $j$ no es constante, para ello nos basta con ver que su discriminante es no constante. El discriminante es

$$\begin{aligned}
&210368365234383038360847215920422164509011148800000\\
&- 7846373837681689005597608965810750639679897057280 0\,T^2\\
&+ 3687451158346283293210344457440165213192253754 88\,T^4\\
&- 2632734019228134900291559382230741736759808 00\,T^6\\
&- 1552767775759515233146125262679384383872 0\,T^8\\
&- 3520549414682181212291260619880038 4\,T^{12}\\
&+ 8102928358247353481991813673813217280 0\,T^{10}\\
&+ 6713802311035606356769402060800\,T^{14}\\
&- 5394389716378326333599907 84\,T^{16}\\
&+ 4536994532332142592 00\,T^{18}\\
&+ 1631591344373760000\,T^{20}.
\end{aligned}$$

□

Por lo tanto $\mathcal{E}_A$ define una familia infinita de curvas elípticas, no isomorfas entre sí, definidas sobre $\mathbb{Q}$ de rango $\geq 13$.

### 7.6.4 Mestre: familia de rango $\geq 13$.

En esta sección vamos a mostrar la construcción, debida a Mestre ([MES7]), de una curva elíptica de rango $\geq 13$ definida sobre $\mathbb{Q}(u, v)(T)$. A partir de esta curva, Fermigier ([FE2]) construye una curva elíiptica definida sobre $\mathbb{Q}$ de rango al menos 22; esto último lo veremos en la sección §7.7.

Utilizando el método desarrollado en la sección §7.6.2 construimos la curva $\mathcal{E}_A$ mediante la 6-upla $A = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6)$, donde

$$\begin{aligned}
\alpha_1 &= u^3v^2 - 2u^2v^3 + uv^4 - u^4 - 2u^2v^2 - 2uv^3 + v^4 + u^2v + uv^2 - v^3 + u^2 + 2uv + v^2 - v,\\
\alpha_2 &= u^4v - 2u^3v^2 + u^2v^3 + u^4 - 2u^3v - 2u^2v^2 - v^4 - u^3 + u^2v + uv^2 + u^2 + 2uv + v^2 - u,\\
\alpha_3 &= u^4 + u^4v - u^3v^2 - 2u^3v - 2u^3 + u^2v^3 + u^2v^2 + u^2 - 2u^2v + 2uv^3 - uv^4 + uv^2 + v^3 - v,\\
\alpha_4 &= u^3 - u^4v - 2u^2v + u^2v^2 + u^2v^3 - 2u^2 - 2uv + uv^2 + 2uv^3 + u - v^2 + v^3 - v^4 + v,\\
\alpha_5 &= u^3v^2 - u^4v + 2u^3v + u^3 + u^2v^2 - u^2v^3 + u^2v - 2uv^3 - 2uv^2 - u + uv^4 - 2v^3 + v^2 + v^4,\\
\alpha_6 &= -\alpha_1 - \alpha_2 - \alpha_3 - \alpha_4 - \alpha_5.
\end{aligned}$$

Con esta 6-upla obtenemos la curva elíptica $\mathcal{E}_A$ definida sobre $\mathbb{Q}(u,v)(T)$. Como vimos en la sección §7.6.2, esta curva tiene al menos 12 puntos. Encontramos un decimotercer punto independiente de los 12 anteriores que tiene como abscisa

$$\frac{A+BT}{u^2+v^2+1}$$

con

$A = 3u^3v^2 + 2u^4v + uv - 4v^3u - 3v^2u^2 + 3v^3u^2 - 4u^3v + u + v - u^6 + v^3 - 3v^4$
$+ 2v^5 - v^6 + 3u^2v + 3v^2u + 2v^4u - 3u^4 + u^3 + 2u^5 + u^5v^2 + u^5v - u^4v^3$
$- 2u^4v^2 - u^3v^4 - 4u^3v^3 + u^2v^5 - 2u^2v^4 + uv^5,$
$B = -u^2 - v^2 + 2u + 2v + 1.$

$\mathcal{E}_A$ es de la forma

$$Y^2 = R(X),$$

donde $R(X)$ es un polinomio de grado 4 en $X$. Si denotamos por $C_4$ al coeficiente de $X^4$ en $R(X)$ se observa que es de la forma

$$C_4 = C(u,v)^2t^2 + D(u,v)$$

donde $C(u,v), D(u,v) \in \mathbb{Q}[u,v]$. Si parametrizamos la cónica (en (T,u)) $C_4 = u^2$ por $t = f(T)$, obtenemos una familia de dos parámetros $(u,v)$ de curvas elípticas definidas sobre $\mathbb{Q}(T')$ de rango $\geq 13$. Para ver esto último basta con observar que la curva construida por Nagao en la sección §7.6.3 se obtiene de ésta mediante las especialización $(u,v) = (2,5)$, que es un homomorfismo.

**Observación 7.6.16** Recientemente, Mestre ha encontrado una familia infinita de curvas elípticas definidas sobre $\mathbb{Q}(T)$ de rango $\geq 14$. Este resultado será publicado a principios de 1998.

## 7.7 Curvas elípticas de rango alto sobre $\mathbb{Q}$.

Vamos a ver dos de los ejemplos de curvas elípticas definidas sobre $\mathbb{Q}$ más significativos de los últimos años. Por una parte, un ejemplo de Nagao con el que consigue una curva elíptica de rango $\geq 21$ y el actual récord debido a Fermigier, que obtiene una de rango $\geq 22$.

### 7.7.1 Nagao: rango $\geq 21$.

En esta sección vamos a mostrar la existencia de una curva elíptica definida sobre $\mathbb{Q}$ de rango al menos 21 entre las curvas obtenidas por especialización de las de rango alto definidas sobre $\mathbb{Q}(T)$ construidas a partir del método de Mestre de la sección §7.6.2. Nagao ([N-K]) consiguió esta curva usando la súper computadora Hitachi Hitac S-820.

Sea $A = (399, 380, 352, 47, 4, 0)$. Entonces tenemos $c_5 = 0$. Tomando una cierta ecuación de Weierstrass $\mathcal{E}_{Wei,A}$ de $\mathcal{E}_A$, tenemos

$$S(563, \mathcal{E}_{Wei,A}) \geq 10.$$

Sea $E_{t_1/t_2}$ la curva obtenida de $\mathcal{E}_{Wei,A}$ por la especialización $T \to t_1/t_2$. Buscamos $t_1, t_2, N \in \mathbb{N}$ tales que $1 \leq t_1 \leq 20000,\ 1 \leq t_2 \leq 2000$, y $s_{Nagao}(N, E_{t_1/t_2})$ sea suficientemente grande. Y encontramos que para $t_1 = 14721, t_2 = 376$ y $N = 6581$ se tiene

$$s_{Nagao}(6581, E_{14721/376}(\mathbb{Q})) \geq 20.$$

De hecho se va a tener que el rango de $E_{14721/376}(\mathbb{Q})$ es $\geq 21$. Así obtenemos el siguiente resultado:

**Teorema.** *Sea $E$ la curva elíptica*

$$y^2 + xy + y = x^3 + x^2 - 215843772422443922015169952702159835x - 19474361277787151947255961435459054151501792241320535,$$

*y sean $P_1, \ldots, P_{21}$ dados por*

$P_1 = (800843008889340065933/16, 22662214190910903990783584765347/64),$
$P_2 = (106105410667639145906372209, 10877441148251784548400947947780341038232),$
$P_3 = (907186946780634143, 728916386168451830641677698),$
$P_4 = (19683320108556444219408310722791940 9, 22778073989304408195874101847939237638943440899317673),$
$P_5 = (18546347413906465252800007 5/366301321, 22569985783858324284947383046648197814670106409826 19),$
$P_6 = (-12485261071234691432503/123904, 15433033534289399822821717527025394361420 8),$
$P_7 = (-59703014087684747037/361, 74188124509415406852503612696 2/6859),$
$P_8 = (-73270463404799613067/361, 86687813785863879289111794348 2/6859),$
$P_9 = (-360733396398627565, 10698584048409672894788397 4),$
$P_{10} = (-389445180957906897, 74288355118790673852542098),$
$P_{11} = (-14744583503498585126654 07/14205361, 22784934015783680843104090282593326 32/53540005609),$
$P_{12} = (-11430585603546889269177927 7/278589481, 16972779768877136292841029639987095378/4649937027371),$
$P_{13} = (-21972533600828202797/81, 10079078658496350456387600530 2/729),$
$P_{14} = (-25047938415396324842058977/71216721, 68347192566984943007522052612937752062/600997908519),$
$P_{15} = (34348280818851183522137152847 07/5137262501809, 42799124838389250442349391653296975768124338 46/11643877735262694377),$
$P_{16} = (-227656313261676647, 13366002432726894909529779 8),$
$P_{17} = (-40980894341059921378352 93/12552849, 56600884139913517593014036598908897 06/44474744007),$
$P_{18} = (26578287358691780202126 17/1495729, 41744997315499971865961317212732013 76/1829276567),$

$P_{19} = (883965004314243424124994323/850947241,$
$232500779860022149171450417087212768121 78/24822981967211),$
$P_{20} = (37543938954172817209003/73441,$
$122409791599128009990383549002029 8/19902511),$
$P_{21} = (19165312347502458410162233/17214201,$
$755938398157414854503489970555516949 52/71421719949).$

*Entonces,*

$$rango\, E(\mathbb{Q}) \geq 21$$

*y* $P_1, \ldots, P_{21}$ *son puntos independientes en* $E(\mathbb{Q})$.

*Demostración:* Usando el paquete APECS ([APECS]) de MAPLE obtenemos que $E_{14721/376}$ es $\mathbb{Q}$-isomorfa a $E$. Usando el sistema de cálculo PARI, tenemos que el determinante de la matriz

$$(< P_i, P_j >)_{1 \leq i,j \leq 21}$$

asociada a la altura canónica es

$$105766268306165799807988 7.489.$$

Como el determinante es distinto de cero, vemos que los puntos $P_1, ..., P_{21}$ son independientes.

□

### 7.7.2 Fermigier: rango $\geq 22$.

A partir de la curva elíptica definida sobre $\mathbb{Q}(u, v)(T)$ de rango $\geq 13$ construida por Mestre, que vimos en la sección 7.6.4, Fermigier encuentra una curva elíptica definida sobre $\mathbb{Q}$ de rango al menos 22. Para los cálculos, Fermigier usó unas decenas de estaciones de trabajo Sparc a lo largo de una semana.

**Teorema.** *Sea* $E$ *la curva elíptica*

$E : y^2 + xy + y = x^3 - 940299517776391362903023121165864x$
$+ 10707363070719743033425295515449274534651125011362$

*y sean* $P_1, \ldots, P_{22}$*:*

$P_1 = (32741153161482344264/3025,$
$-22308967458711097957853216 9697/166375),$
$P_2 = (215521674613198983365/24649,$
$-68729491550613535423570437 8947/3869893),$
$P_3 = (637312541911044643/81, -14203561901292968321935640 87/729,$
$P_4 = (-11906250919327880080/361, -16580788535875788634285886853/6859)$
$, P_5 = (-136152345735493381/4, -14482270545045735913281693/8),$
$P_6 = (-27830298157016213012252/7134241,$
$720996928613643927961833594974542 67/19055557711),$
$P_7 = (4127671322151440, 26261076920456131162916 46),$
$P_8 = (6175679781777296, 22662543359970331246784 49),$

$P_9 = (12047255022287093, 1061993236525943920980477)$,
$P_{10} = (416685837455186583191/32761,$
$532126822278670966916031158736 9/5929741)$,
$P_{11} = (14991581313907576710802 4/10220809,$
$87043268381086469491776631579171 17/32675926373)$,
$P_{12} = (58759417448623559/4, 2030968553150713398654657/8)$,
$P_{13} = (237195157887349854919517/16024009,$
$-1147779811161130797970721550542 1441/64144108027)$,
$P_{14} = (9568474434078537574436/687241,$
$319520556343135681977874272805086/569722789)$,
$P_{15} = (1725892668710258675291/177241,$
$1173780506634648457709664530250 39/74618461)$,
$P_{16} = (-35277008506980340471/1024,$
$4876602714394693418673167450 7/32768)$,
$P_{17} = (-2752742763529705669/121,$
$600053225218598238123358569 9/1331)$,
$P_{18} = (-18552633109178014, -4665466215824339436717966)$,
$P_{19} = (-113251707338691187737649969/3304065361,$
$3101525278948314708200098723732293 41739/189920981015641)$,
$P_{20} = (-7572001778163591251/729, -865906614265067993576635029 53/19683)$,
$P_{21} = (-380526048554032285152211/11242609,$
$730812357449313076847906230684902 33/37696467977)$,
$P_{22} = (-150388949772202158811068 1/42784681,$
$-1607058851701167501515346409247 19585/279854598421)$

*Entonces,*

$$rango\, E(\mathbb{Q}) \geq 22$$

*y* $P_1, \ldots, P_{22}$ *son puntos independientes en* $E(\mathbb{Q})$.

*Demostración:* De acuerdo con el sistema de cálculo PARI, $E$ es

```
E=initell([1, 0, 1, -940299517776391362903023121165864,
107073630707197430334252955154492745346511250113 62]);
```

Usando el sistema de cálculo PARI tenemos que el determinante de la matriz, denotando por $Pi := P_i$,

$$(< Pi, Pj >)_{1 \leq i,j \leq 22}$$

asociado a la altura canónica es, en el lenguaje de PARI:

```
m=mathell(E,[P1,P2,P3,P4,P5,P6,P7,P8,P9,P10,P11,P12,P13,
P14,P15,P16,P17,P18,P19,P20,P21,P22]);
m=12992022722213680254541.34536.
```

Por lo tanto vemos que $P1, \ldots, P22$ son puntos independientes, ya que el determinante anterior es no nulo.

□

# Bibliografía


[A-M] M.F. Atiyah y I.G. Macdonald *Introducción al álgebra conmutativa*.Editorial Reverté, 1973.

[ABR] D. Abramovich, *Formal finiteness and the torsion conjecture on elliptic curves. A footnote to a paper: "Rational torsion of prime order in elliptic curves over number fields "*. Asterisque **228** 3 (1995), 5-17.

[APECS] I. Connell, *Arithmetic of Plane Elliptic CurveS*. Se puede encontrar en `ftp://math.mcgill.ca/pub/apecs/`, 1995.

[BEA] A. Beauville, *Complex Algebraic Surfaces*. London Math. Soc., LNS 68, 1983.

[B-K] A. Brumer y K. Kramer, *The rank of elliptic curves*. Duke Math. J., **44** (1977),715-743.

[B-M] A. Brumer y O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*. Bulletin of the AMS **23** (1990), 375-382.

[B-P-V] W. Barth, C. Peters y A. Van de Ven, *Compact Complex Surfaces*. A Series of Modern Surveys in Mathematics, Springer-Verlag, 1984.

Springer-Verlag, 1975.

[B-S-D] B. Birch y H. P. F. Swinnerton-Dyer, *Notes on elliptic curves (I),(II)*. J. Reine Angew. Math **212** (1963), 7-25 y **218** (1965), 79-108.

[CAS] J.W.S. Cassels, *Lectures on Elliptic Curves*. London Math. Soc., Student Texts **24**, 1991.

[C-C] J. Cilleruelo y A. Cordoba, *La Teoría de los Números*. Biblioteca Mondadori, 1992.

[C-W] J. Coates y A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*. Invent. Math. **39** (1977), 223-251.

[DEL] P. Deligne, *La conjecture de Weil*. Publ. Math. IHES **43** (1974), 273-307.

[DWO] B. Dwork, *On the rationality of the zeta function of an algebraic variety*. Amer. J. of Math. **82** (1960), 631-648.

[EDI] B. Edixhoven, *Rational torsion points on elliptic curves over number fields*. Astérisque, Séminaire Bourbaki 782, 46éme année, 1993-94.

[FAL1] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpen*. Invent. Math. **73** (1983), 349-366. Se puede encontrar una traducción al inglés en el Capítulo 2 de: G. Cornell y J. H. Silverman eds., *Arithmetic Geometry*. Springer-Verlag, 1986.

[FAL2] G. Faltings, *The general case of S. Lang's conjecture*. Proccedings of the Barsotti symposium in algebraic geometry, Academic Press, San Diego, 1994.

[FE1] S. Fermigier, *Un example de courbe elliptique définie sur* $\mathbb{Q}$ *de rang* $\geq 19$. C.R. Acad. Sci. Paris **315**, Série I (1992), 719-722.

[FE2] S. Fermigier, *An elliptic curve over* $\mathbb{Q}$ *of rank* $\geq 22$. Se puede encontrar en `http://www.math.jussieu.fr/~fermigie/elliptic.html.en`, 19 Mayo 1996.

[FRE] G. Frey, *Curves with manitely many points of fixed degree*. Israel J. Math. **85** (1994), 79-83.

[GOL] D.Goldfeld, *Gauss class number problem for imaginary quadratic fields*. Bulletin of the AMS **13** (1985), 23-37.

[G-Z1] B. Gross y D. Zagier, *Points de Heegner et dérivées de fonctions L*. C. R. Acad. Sci. Paris **297** (1983), 85-87.

[G-Z2] B. Gross y D. Zagier, *Heegner points and derivatives of L-functions*. Invent. Math. **84** (1986), 225-320.

[G-ZI] F, J. Grunewald y R. Zimmert, *Über einige rationale elliptische Kurven mit freiem Rang* $\geq 8$. Journal Reine u. Angew. Math. **296** (1977), 100-107.

[GRI] P.A. Griffiths, *Introduction to Algebraic Curves*. AMS, 1989.

[HAR] R. Hartshorne, *Algebraic Geometry*. Springer-Verlag, 1977.

[HER] E. Hernández, *Álgebra y Geometría*. Ediciones de la U.A.M., 1987.

[I-R] K. Ireland y M. Rosen, *A classical introduction to modern number theory*. Second edition. Graduate text in Math., Springer-Verlag, 84, New York, 1972.

[KAM] S. Kamienny, *Torsion Points on Elliptic Curves and q-cofficients of modular forms*. Invent. Math. **109**, No. 2 (1992), 221-229.

[K-M] S. Kamienny y B. Mazur, *Rational Torsion of prime orden in elliptic curves over number fields*. Asterisque **228**, 3 (1995), 81-100.

[KE-MO] M. Kenku y F. Momose, *Torsion points on elliptic curves defined over quadratic fields*. Nagoya Mathematical Journal **109** (1988), 125-149.

[KIR] F. Kirwan, *Complex Algebraic Curves*. Cambridge Univiversity Press, 1992.

[KNA] A.W. Knapp, *Elliptic Curves*. Princeton U. P., 1992.

[KOB] N. Koblitz, *A course in Number Theory and Cryptography*. Springer-Verlag. Graduate Texts in Math. 114. Segunda edición, 1994.

[KOL1] V. A. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $Ш(E/\mathbb{Q})$ *for a class of Weil curves*. Izv. Akad. Nauk. SSSR 52, 1988.

[KOL2] V. A. Kolyvagin, *Euler systems*. The Grothendieck Festschrift Volume 2. Birkhäuser, 435-483, 1990.

[LAN] S. Lang, *Fundamentals of Diophantine Geometry*. Springer-Verlag, 1983.

[LUT] E. Lutz, *Sur l'equation* $y^2 = x^3 - Ax - B$ *dans les corps p-adic*. J. Reine Angew. Math. **177** (1937), 237-247.

[MAZ1] B. Mazur, *Modular curves and the Einsenstein Ideal*. I.H.E.S. Publ. Math. **47** (1977), 33-186.

[MAZ2] B. Mazur, *Rational Isogenies of Prime degree*. Invent. Math. **44** No. 2 (1978), 129-162.

[MER] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math. **124** (1996), 437-449.

[MES1] J.-F. Mestre, *Courbes elliptiques de rang* $\geq 11$ *sur* $\mathbb{Q}(t)$. C.R. Acad. Sci. Paris **313**, série I (1991), 139-142.

[MES2] J.-F. Mestre, *Courbes elliptiques de rang* $\geq 12$ *sur* $\mathbb{Q}(t)$. C.R. Acad. Sci. Paris **313**, série I (1991), 171-174.

[MES3] J.-F. Mestre, *Un example de courbe elliptique sur* $\mathbb{Q}$ *de rang* $\geq 15$. C.R. Acad. Sci. Paris **314**, série I (1992), 453-455.

[MES4] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variété algébraiques*. Compositio Math. **58** (1986), 209-232.

[MES5] J.-F. Mestre, *Construction de courbes elliptiques de rang* $\geq 12$ *sur* $\mathbb{Q}$. C.R. Acad. Sci. Paris **295**, série I (1982), 643-644.

[MES6] J.-F. Mestre, *Courbes elliptiques et formules explicites*. Sém. Th. Nombres, Paris 1981-82. Progress in Math. 38, Birkhäuser, 179-188.

[MES7] J.-F. Mestre, *Constructions polynomiales et théorie de Galois*. Proccedings of the International Congress of Mathematicians. Zürich, Birkhäuser Verlag, Basel, 318-323, 1995.

[MOR1] L.J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*. Proc. Camb. Philos. Soc. **21** (1922), 179-192.

[MOR2] L.J. Mordell, *Diophantine Equation*. Academic Press, 1968.

[NA1] K. Nagao, *Examples of elliptic curves over* $\mathbb{Q}$ *with rank* $\geq 17$. Proc. Japan Acad. **68**, Serie A (1992), 287-289.

[NA2] K. Nagao, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* $\geq 20$. Proc. Japan Acad. **69**, Serie A (1993), 291-293.

[NA3] K. Nagao, *An example of elliptic curve over* $\mathbb{Q}(T)$ *with rank* $\geq 13$. Proc. Japan Acad. **70**, Serie A (1994), 152-153.

[NA4] K. Nagao, $\mathbb{Q}(T)$*-rank of elliptic curves and certain limit coming from the local points*. Manuscripta Math. **92** (1997), 13-32.

[NA5] K. Nagao, *On the Mordell-Weil rank of elliptic curves*. Tesis Doctoral, 1995.

[N-K] K. Nagao y T. Kouya, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* $\geq 21$. Proc. Japan Acad. **70**, Serie A (1994), 104-105.

[NAG1] T. Nagell, *Sur les propetés arithmétiques des cubiques planes du premier genre*. Acta Math. **52** (1928-9), 92-108.

[NAG2] T. Nagell, *Solution de quelque problémes dans la théorie arithmétique des cubiques planes du premier genre*. Wid. Akad. Skrifter Oslo I, No.1, 1937.

[NER1] A. Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang dúne courbe algébrique dans un corps*. Bull. Soc. Math. France **80** (1952), 101-166.

[NER2] A. Néron, *Propriétés arithmétique de certaines familles de courbes algébriques*. Proc. Intern. Congress Amsterdam, vol. **3** (1954), 481-488.

[NIS] K. Nishioka (K. Nakata), *On some elliptic curves defined over* $\mathbb{Q}$ *of free rank* $\geq 9$. Manu. Math. **29** (1979), 183-194.

[PAR] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*. Preprint IRMAR. Se puede encontrar en `http://eprints.math.duke.edu/abs/alg-geom/9604003`, 1996.

[PARI] C. Batut, D. Bernardi, H. Cohen, M. Olivier, *PARI-GP, a computer system for number theory, Version 1.39*. Se puede encontrar en `ftp://megrez.math.u-bordeux.fr`, 1995.

[P-P1] D. E. Penney y C. Pomerance, *A search for elliptic curves with large rank*. Math. Comp. **28** (1974), 851-853.

[P-P2] D. E. Penney y C. Pomerance, *Three elliptic curves with large rank at least seven*. Math. Comp. **29** (1975), 965-967.

[RIB] K. Ribet, *From the Taniyama-Shimura conjecture to Fermat's last theorem*. Ann. Fac. Sci. Toulouse Math. Serie 5, **11** (1990), 116-139.

[ROB] A. Robert, *Elliptic Curves*. Lectures Notes in Math. **326**, Springer-Verlag, 1973.

[RUB] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complec multiplication*. Invent. Math. **89** (1987), 527-560.

[R-S] M. Rosen y J.H. Silverman, *On the rank of an elliptic surface*. Se puede encontrar en `http://jacobi.math.brown.edu/~jhs/Preprints/`, 1997.

[SEL] E. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$. Acta. Math. **85** (1951), 203-362 y **92** (1954), 191-197.

[SAM] P. Samuel, *Teoría Algebraica de Números*. Ediciones Omega, 1972.

[SHA] I.R. Shafarevich, *Basic Algebraic Geometry*. Springer-Verlag, 1977.

[SHI] T Shioda, *On the Mordell-Weil Lattices*. Comm. Math. Univ. Sancti Pauli. **39** (1990), 211-240.

[SI] A. Silverberg, *Points of finite order on abelian varieties*. p-Adic Methods in Number Theory and Algebraic Geometry, Contemporary Mathematics **133** (1992), 175-193.

[SIL] J.H. Silverman, *The Arithmetic of Elliptic Curves*. Graduate Texts in Math. 106, Springer-Verlag, New York, 1986.

[SIL2] J.H. Silverman, *Advanced topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Math. 151, Springer-Verlag, New York, 1994.

[SIL3] J.H. Silverman, *The average rank of an algebraic family of elliptic curves*. Se puede encontrar en `http://jacobi.math.brown.edu/~jhs/Preprints/`, 1997.

[SH-T] I.R. Shafarevich y J. Tate, *The rank of elliptic curves*. AMS. Transl. **8** (1967), 917-920.

[SI-T] J.H. Silverman y J. Tate, *Rational points on elliptic curves*. Springer-Verlag, New York, 1992.

[S-T] I. Stewart y D. Tall, *Algebraic Number Theory*. Chapman and Hall, London, 1987.

[TAT] J. Tate, *Algebraic cycles and poles of zeta functions*. Arithmetic Algebraic Geometry, ed. Schlling, Harper and Row, (1965), 93-111.

[WE1] A. Weil, *L'arithmétique sur les courbes algébriques*. Acta Math. **52** (1928), 281-315.

[WE2] A. Weil, *Sur un théoreme de Mordell*. Bull. Sci. Math. **54** (1930), 182-191.

[WE3] A. Weil, *Number of solutions of equations in finite fields*. Bull. AMS **55** (1949), 497-508.

[WIL] A. Wiles, *Modular elliptic curves and Fermat's last theorem*. Annals of Math. **141** (1995), 443-551.

[WMLI] M. Waldschmidt, P. Moussa, J.M. Luck y C. Itzykson eds., *From Number Theory to Physics*. Springer-Verlag, 1989.